STATE OF PLAY: FEDERAL IT IN 2018

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

AND THE

SUBCOMMITTEE ON
GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

MARCH 14, 2018

Serial No. 115–75

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
31–105 PDF WASHINGTON : 2018

Committee on Oversight and Government Reform

Trey Gowdy, South Carolina, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan
Greg Gianforte, Montana

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Jimmy Gomez, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
Stacey E. Plaskett, Virgin Islands
John P. Sarbanes, Maryland

Sheria Clarke, *Staff Director*
William McKenna, *General Counsel*
Meghan Green, *Counsel*
Troy Stock, *Information Technology Subcommittee Staff Director*
Julie Dunne, *Government Operations Subcommittee Staff Director*
Sharon Casey, *Deputy Chief Clerk*
David Rapallo, *Minority Staff Director*

Subcommittee on Information Technology

Will Hurd, Texas, *Chairman*

Paul Mitchell, Michigan, *Vice Chair*
Darrell E. Issa, California
Justin Amash, Michigan
Steve Russell, Oklahoma
Blake Farenthold, Texas
Greg Gianforte, Montana

Robin L. Kelly, Illinois, *Ranking Minority Member*
Jamie Raskin, Maryland
Stephen F. Lynch, Massachusetts
Gerald E. Connolly, Virginia
Raja Krishnamoorthi, Illinois

Subcommittee on Government Operations

Mark Meadows, North Carolina, *Chairman*

Jody B. Hice, Georgia, *Vice Chair*
Jim Jordan, Ohio
Mark Sanford, South Carolina
Thomas Massie, Kentucky
Ron DeSantis, Florida
Dennis A. Ross, Florida
Rod Blum, Iowa

Gerald E. Connolly, Virginia, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey

CONTENTS

STATE OF PLAY: FEDERAL IT IN 2018

Wednesday, March 14, 2018

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY, JOINT
WITH THE SUBCOMMITTEE ON GOVERNMENT OPERATIONS,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittees met, pursuant to call, at 3:16 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the Subcommittee on Information Technology] presiding.

Present from the Subcommittee on Information Technology: Representatives Hurd, Gianforte, Kelly, and Krishnamoorthi.

Present from the Subcommittee on Government Operations: Representatives Hice, Blum, Connolly, and Maloney.

Mr. HURD. The Subcommittee on Information Technology and the Subcommittee on Government Operations will come to order.

And, without objection, the presiding member is authorized to declare a recess at any time.

Good afternoon. Sorry for the wait, but it is Washington, D.C. And the House of Congress is the people's House, but sometimes we get a little delayed.

We have had momentum over the last couple years. I think this year, or this Congress, with the Federal IT modernization effort through the passage of the MGT Act, the Modernizing Government Technology Act, we have gained strength and force. This, now a law, is bipartisan legislation that will, for the first time, reward and incentivize Federal agencies and CIOs to cut costs and invest in cutting-edge technology.

The effort, also, of modernization has gained momentum from Trump administration initiatives like establishing the Office of American Innovation, releasing an IT modernization report, and retaining good ideas from the previous administration, including the U.S. Digital Service.

I am concerned, however, that in some areas we have lost momentum. We went too long without a Federal CIO. I am glad Ms. Kent is now in the position and look forward to having her up here before the committee within the next few months.

I am also pleased that Ms. Weichert is in place as the Deputy Director for Management at OMB.

I have spoken to my former colleague, Director Mulvaney, about our efforts here in the subcommittee and how we can work together to modernize government. He is an enthusiastic supporter of using emerging technologies to make government more efficient and accountable.

We need to rethink how we structure the Federal workforce, to ensure the Federal Government has access to smart, well-trained IT and cybersecurity professionals, and be working in a bipartisan fashion, as always, in introducing a bill in the coming months to establish the U.S. cyber reserves, a public/private-sector rotational workforce. I look forward to the witnesses' thoughts on how to best organize and structure this kind of workforce.

I also continue to have concerns about longstanding GAO recommendations that remain unaddressed, oftentimes year after year after year. These open, lingering vulnerabilities put us at incredible risk, as we saw with the devastating data breach at OPM, which it is crazy to think was almost 3 years ago.

I want to hear from GAO their most critical open recommendations and, from the rest of the witnesses, concrete plans to close them. Let's use this hearing to ensure IT modernization across the Federal Government continues, even with more force and strength, in 2018. Let's not lose the momentum.

And, as always, it is an honor to be exploring these very important issues in a bipartisan fashion with my friend, the ranking member, the one and only, the Honorable Robin Kelly from Illinois.

Ms. KELLY. Thank you, Mr. Chairman. Thank you for calling today's hearing on the Federal Government's information technology.

These two subcommittees have prioritized holding agencies accountable for their compliance with the Federal Information Technology Acquisition Reform Act in the effort to modernize our legacy IT systems. We have managed to work in a bipartisan manner not only to conduct oversight but to introduce legislation seeking to address the Nation's IT and cybersecurity problems.

Improving the efficiency and security of the Federal Government's IT system is essential to our Nation's security. In order to improve the efficiency and security, we must modernize legacy IT systems across every Federal agency.

The Federal Government spends nearly $60 billion just to sustain its existing outdated IT. When agencies must spend 75 percent of their IT budgets merely to maintain legacy systems, they predictably fall behind in the effort to modernize.

That is why the Modernizing Government Technology Act of 2017 is critical to shoring up our Nation's cybersecurity and moving us forward. MGT is now law. It creates a working capital fund called the Technology Modernization Fund that will have money for efforts like cloud migration for agency CIOs to think creatively about modernization.

The next couple of months will determine whether the MGT Act is allowed to spur that type of innovation. I was pleased to see that the President's proposal budget called for $228 million for the modernization fund. OMB Director Mulvaney recently released a memo to agencies with guidance on MGT's implementation.

The board overseeing the modernization fund is in place. It is now up to Congress to fund this important effort. Our government technology is too outdated to allow this opportunity to pass us by.

By allocating these funds, we further our goals under FITARA to fully empower agency CIOs. I view the MGT Act as a natural complement of FITARA. We cannot speak about important efforts, like moving to the cloud and data center consolidations, without providing the funding necessary to make that happen.

In addition to modernizing our technology, we must modernize our Federal workforce to make sure they have the tools and skills necessary to address the problems of not only today but tomorrow.

In 2016, GAO found that the evolving array of cyber-based threats continue to pose a risk to our national security. The government's inability to attract and retain qualified cyber professionals throughout the government threatens our ability to address these cyber threats. Therefore, attracting IT and cybersecurity talent is critical to the safety of every American and the security of our country.

I hope that our witnesses can update us on the state of the Federal IT and how each agency plans to address the opportunities and challenges facing the Federal Government.

Thank you, Mr. Chairman.

Mr. HURD. Thank you, Ranking Member Kelly.

And when the ranking member and chair of Government Operations get here, we will allow them to have opening remarks, if they do. But now it is a pleasure to introduce our witnesses.

Mr. David Powner, probably our most visits to this committee of anybody in government. Thanks for being here. And he is the Director of IT Management Issues at GAO.

The Honorable Margaret Weichert, Deputy Director for Management at the Office of Management and Budget. Thank you for being here.

Mr. Bill Zielinski, Deputy Assistant Commissioner of the IT Category at the General Services Administration.

And last but not least, the Honorable Jeanette Manfra, Assistant Secretary for the Office of Cybersecurity and Communications at the Department of Homeland Security.

Welcome to you all. And pursuant to committee rules, all witnesses will be sworn in before you testify, so please stand and raise your right hand.

Do you solemnly swear or affirm the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Thank you.

Please let the record reflect that the witnesses answered in the affirmative.

In order to allow time for discussion, please limit your opening remarks to 4 minutes. Your entire written statement will be part of the record.

And as a reminder, the clock in front of you shows the remaining time during your opening statement. The light will turn yellow when you have 30 seconds left and red when your time is up. Please also remember to press the button for the speaker.

So, with that, Mr. Powner, welcome back.

WITNESS STATEMENTS

STATEMENT OF DAVID POWNER

Mr. POWNER. Chairman Hurd, Ranking Member Kelly, and members of the subcommittee, I would like to commend your subcommittee for your consistent and thorough oversight of IT and cybersecurity issues, in particular with FITARA and with recently moving the FITARA Enhancement Act and MGT.

This afternoon, I will highlight top priorities for OMB and agencies. My comments will address three broad areas: human capital, acquisitions, and operations.

CIO authorities still need to be strengthened, despite significant improvements from FITARA. Your push to elevate these positions at departments and agencies is still needed. Currently, 13 of the 24 CIOs report to the DEPSEC or higher. OMB plays a critical role here, especially with the recent focus on agency reorganizations.

Also, cybersecurity and IT workforce needs to be further strengthened. Specifically, we still need to properly identify and tackle our workforce gaps. Properly addressing many of these needs with contractors is a critical part of the solution here. GAO has ongoing government-wide reviews looking at both the cybersecurity and IT workforce needs.

Turning to improvements on major acquisitions, we still need to stay the course with major provisions in FITARA. This starts with incremental development. Your scorecard shows major progress in this area, but we still have too many projects not tackling this in manageable segments.

We also need to have IT shops aware of IT contracts so that we can avoid duplication and to ensure the right governance over these acquisitions. A recent contracting review was discouraging, as only one-third of the agencies had a process to approve IT contracts consistent with FITARA and OMB guidance.

And of our sample of almost 100 contracts, only 10 percent were approved by CIOs or their designee. Strengthening the relationship between CIOs and chief acquisition officers is needed.

We also believe the Nation's top Federal IT acquisitions should have OMB governance over them in addition to agency governance. The top acquisitions should include VA and DOD's EHR acquisitions, IRS's K–2 project, SSA's disability case processing system, and FAA's NextGen acquisitions.

The reason these acquisitions need OMB's attention is because these agencies, left alone, haven't managed them well. The administration's attention to VA's EHR solution is spot-on; we just need more of this. We have a review underway where we are identifying and profiling these most critical acquisitions.

Regarding operational systems, again, we need to stay the course with FITARA. Data center optimization metrics provide great transparency on where agencies are at with their optimization metrics. And extending the sunset date from 2018 to 2020 will give agencies more time to both optimize and save.

A couple key points here: Savings still can be significant as we optimize space and equipment. And the MGT working capital funds can be used to invest in unfunded priorities.

Also, these agencies who can't optimize by 2020 need to get out of the data center business. We plan to report annually through 2020 on agencies' data center progress.

We also believe that the Nation's most mission-critical legacy systems that are costly to maintain and pose significant cyber risk due to unsupported software need to be replaced with modern, secure technologies and ultimately decommissioned.

OMB needs to have an active role here to ensure that these old systems, like VA's VistA system and IRS's Individual Master File, have plans to replace and decommission.

The administration's recent modernization strategy was solid on network modernization, shared services, and cyber but light on tackling these most challenging modernization efforts. CIOs with average tenures of 2 years don't always focus on these longer-term, challenging legacy systems, which is even more reason for OMB to drive this. We have a review underway where we are identifying and profiling these legacy systems most in need of modernization.

In conclusion, the American Tech Council, the Office of Innovation, and the modernization strategy are all positive developments. Now we need more action and implementation from OMB and agencies.

Key focus areas should be on fixing CIO authorities in the IT workforce; regarding acquisitions: incremental development, CIO alignment with acquisitions, and the focus on our Nation's top acquisitions is needed. On the operations side, data center optimization and mission-critical legacy modernization need continued attention.

Finally, the Comptroller General held a forum with prior Federal and agency CIOs from previous administrations in late 2016 to explore what has worked over the years in Federal IT. The results of this forum, summarized on page 10 of my written statement, are consistent with the comments here this afternoon and highlight the critical role OMB leadership plays.

Mr. Chairman, again, thank you for your oversight of Federal IT.

[Prepared statement of Mr. Powner follows:]

United States Government Accountability Office

GAO

Testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, March 14, 2018

INFORMATION TECHNOLOGY

Further Implementation of Recommendations Is Needed to Better Manage Acquisitions and Operations

Statement of David A. Powner, Director
Information Technology Management Issues

GAO
Highlights

Highlights of GAO-18-460T, a testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Government Reform, House of Representatives

March 14, 2018

INFORMATION TECHNOLOGY

Further Implementation of Recommendations Is Needed to Better Manage Acquisitions and Operations

Why GAO Did This Study

The federal government plans to invest almost $96 billion in IT in fiscal year 2018. Historically, these investments have too often failed, incurred cost overruns and schedule slippages, or contributed little to mission-related outcomes. In December 2014, Congress and the President enacted FITARA, aimed at improving covered agencies' acquisitions of IT. Further, in February 2015, GAO added improving the management of IT acquisitions and operations across government to its high-risk list.

This statement summarizes agencies' progress in improving the management of IT acquisitions and operations. Among others, GAO summarized its published reports on (1) data center consolidation, (2) incremental software development practices, (3) IT acquisitions, (4) IT workforce, and (5) legacy IT.

What GAO Recommends

From fiscal years 2010 through 2015, GAO made about 800 recommendations to OMB and federal agencies to address shortcomings in IT acquisitions and operations. Among other recommendations, GAO made recommendations to improve the oversight and execution of the data center consolidation initiative, incremental development policies, the review and approval of IT acquisitions, implementation of key workforce planning activities, and aging federal IT systems. Most agencies agreed with GAO's recommendations. In addition, from fiscal year 2016 to present, GAO has made more than 200 new recommendations in this area. GAO will continue to monitor agencies' implementation of these recommendations.

View GAO-18-460T. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

The Office of Management and Budget (OMB) and federal agencies have taken steps to improve the management of information technology (IT) acquisitions and operations through a series of initiatives, to include (1) data center consolidation, (2) implementation of incremental development practices, (3) approval of IT acquisitions, (4) implementation of key IT workforce practices, and (5) addressing aging legacy IT systems. As of March 2018, the agencies had fully implemented about 59 percent of the approximately 800 related recommendations that GAO made during fiscal years 2010 through 2015. However, important additional actions are needed.

- **Consolidating data centers**. OMB launched an initiative in 2010 to reduce data centers, which was codified and expanded by a law commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA). GAO has since noted that, while this initiative could potentially save the government billions of dollars, weaknesses exist in areas such as optimization and OMB's reporting on related cost savings. Accordingly, GAO has made 160 recommendations to OMB and agencies to improve the initiative; however, about half of GAO's recommendations have not yet been implemented.
- **Implementing incremental development**. OMB has emphasized the need for agencies to deliver investments in smaller increments to reduce risk and deliver capabilities more quickly. Further, GAO has issued reports highlighting actions needed by OMB and agencies to improve their implementation of incremental development. In these reports, GAO made 42 related recommendations, but the majority of GAO's recommendations have not yet been addressed.
- **Approval of IT acquisitions**. OMB's FITARA implementation guidance required covered agencies' chief information officers (CIO) to review and approve IT acquisition plans. In January 2018, GAO reported that many agencies' CIOs were not reviewing and approving acquisition plans, as required by OMB. GAO made 39 recommendations to improve the review and approval of IT acquisitions, but they have not yet been implemented by the agencies.
- **Implementation of key IT workforce practices**. Effective IT workforce planning can help agencies improve their ability to acquire IT. In November 2016, GAO reported on agencies' IT workforce planning activities. GAO noted that five selected agencies had not fully implemented key workforce planning activities and recommended that they do so, but the agencies have not yet addressed the recommendations.
- **Addressing aging legacy IT systems.** Legacy IT investments across the federal government are becoming increasingly obsolete and consuming an increasing amount of IT dollars. In May 2016, GAO reported that many agencies were using systems which had components that were, in some cases, at least 50 years old. GAO noted, however, that several agencies did not have specific plans with time frames to modernize or replace these investments. GAO recommended that 12 agencies plan to modernize or replace legacy systems; all of which have not yet been implemented.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees:

I am pleased to be here today to provide an update on federal agencies' efforts to improve the acquisition of information technology (IT). As I have previously testified, the effective and efficient acquisition of IT has been a long-standing challenge in the federal government.[1] In particular, the federal government has spent billions of dollars on failed and poorly performing IT investments, which often suffered from ineffective management. Recognizing the severity of issues related to the government-wide acquisition of IT, in December 2014, Congress and the President enacted federal IT acquisition reform legislation (commonly referred to as the Federal Information Technology Acquisition Reform Act, or FITARA).[2]

In addition, in February 2015, we added improving the management of IT acquisitions and operations to our list of high-risk areas for the federal government.[3] We recently issued an update to our high-risk report and noted that, while progress has been made in addressing the high-risk area of IT acquisitions and operations, significant work remains to be completed.[4]

My statement today provides an update on agencies' progress in improving the management of IT acquisitions and operations. The statement is based on our prior and recently published reports that discuss federal agencies' (1) data center consolidation efforts, (2) risk levels of major investments as reported on the Office of Management and Budget's (OMB) IT Dashboard, (3) implementation of incremental

[1] GAO, *Information Technology: Further Implementation of FITARA Related Recommendations Is Needed to Better Manage Acquisitions and Operations*, GAO-18-234T (Washington, D.C.: Nov. 15, 2017).

[2] Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-3450 (Dec. 19, 2014).

[3] GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[4] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

development practices, (4) management of software licenses, (5) approval of IT acquisitions, (6) implementation of key IT workforce practices, and (7) efforts to address aging legacy IT. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

We conducted the work upon which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

According to the President's budget, the federal government plans to invest more than $96 billion for IT in fiscal year 2018—the largest amount ever budgeted. However, as we have previously reported, investments in federal IT too often result in failed projects that incur cost overruns and schedule slippages, while contributing little to the desired mission-related outcomes. For example:

- The Department of Veterans Affairs' Scheduling Replacement Project was terminated in September 2009 after spending an estimated $127 million over 9 years.[5]
- The tri-agency[6] National Polar-orbiting Operational Environmental Satellite System was disbanded in February 2010 by the White House's Office of Science and Technology Policy after the program spent 16 years and almost $5 billion.[7]

[5] GAO, *Information Technology: Management Improvements Are Essential to VA's Second Effort to Replace Its Outpatient Scheduling System*, GAO-10-579 (Washington, D.C.: May 27, 2010).

[6] The weather satellite program was managed jointly by the Department of Commerce's National Oceanic and Atmospheric Administration, Department of Defense, and National Aeronautics and Space Administration.

[7] See, for example, GAO, *Polar-Orbiting Environmental Satellites: With Costs Increasing and Data Continuity at Risk, Improvements Needed in Tri-agency Decision Making*, GAO-09-564 (Washington, D.C.: June 17, 2009) and *Environmental Satellites: Polar-Orbiting Satellite Acquisition Faces Delays; Decisions Needed on Whether and How to Ensure Climate Data Continuity*, GAO-08-518 (Washington, D.C.: May 16, 2008).

- The Department of Homeland Security's Secure Border Initiative Network program was ended in January 2011, after the department obligated more than $1 billion for the program.[8]
- The Office of Personnel Management's Retirement Systems Modernization program was canceled in February 2011, after the agency had spent approximately $231 million on its third attempt to automate the processing of federal employee retirement claims.[9]
- The Department of Veterans Affairs' Financial and Logistics Integrated Technology Enterprise program was intended to be delivered by 2014 at a total estimated cost of $609 million, but was terminated in October 2011.[10]
- The Department of Defense's Expeditionary Combat Support System was canceled in December 2012 after spending more than a billion dollars and failing to deploy within 5 years of initially obligating funds.[11]

Our past work found that these and other failed IT projects often suffered from a lack of disciplined and effective management, such as project planning, requirements definition, and program oversight and governance. In many instances, agencies had not consistently applied best practices that are critical to successfully acquiring IT.

[8] See, for example, GAO, *Secure Border Initiative: DHS Needs to Strengthen Management and Oversight of Its Prime Contractor,* GAO-11-6 (Washington, D.C.: Oct. 18, 2010); *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340 (Washington, D.C.: May 5, 2010); and *Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk*, GAO-10-158 (Washington, D.C.: Jan. 29, 2010).

[9] See, for example, GAO, *Office of Personnel Management: Retirement Modernization Planning and Management Shortcomings Need to Be Addressed,* GAO-09-529 (Washington, D.C.: Apr. 21, 2009) and *Office of Personnel Management: Improvements Needed to Ensure Successful Retirement Systems Modernization*, GAO-08-345 (Washington, D.C.: Jan. 31, 2008).

[10] GAO, *Information Technology: Actions Needed to Fully Establish Program Management Capability for VA's Financial and Logistics Initiative*, GAO-10-40 (Washington, D.C.: Oct. 26, 2009).

[11] GAO, *DOD Financial Management: Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals,* GAO-12-134 (Washington, D.C.: Feb. 28, 2012) and *DOD Business Transformation: Improved Management Oversight of Business System Modernization Efforts Needed,* GAO-11-53 (Washington, D.C.: Oct. 7, 2010).

Such projects have also failed due to a lack of oversight and governance. Executive-level governance and oversight across the government has often been ineffective, specifically from chief information officers (CIO). For example, we have reported that some CIOs' roles were limited because they did not have the authority to review and approve the entire agency IT portfolio.[12]

Implementing FITARA Can Improve Agencies' Management of IT

FITARA was intended to improve covered agencies' acquisitions of IT and enable Congress to monitor agencies' progress and hold them accountable for reducing duplication and achieving cost savings. The law includes specific requirements related to seven areas.[13]

- **Federal data center consolidation initiative (FDCCI).** Agencies covered by FITARA are required to provide OMB with a data center inventory, a strategy for consolidating and optimizing their data centers (to include planned cost savings), and quarterly updates on progress made. The law also requires OMB to develop a goal for how much is to be saved through this initiative, and provide annual reports on cost savings achieved.
- **Enhanced transparency and improved risk management.** OMB and covered agencies are to make detailed information on federal IT investments publicly available, and agency CIOs are to categorize their investments by level of risk. Additionally, in the case of major IT investments[14] rated as high risk for 4 consecutive quarters, the law requires that the agency CIO and the investment's program manager

[12] GAO, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management*, GAO-11-634 (Washington, D.C.: Sept. 15, 2011).

[13] The provisions apply to the agencies covered by the Chief Financial Officers Act of 1990, 31 U.S.C. § 901(b). These agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development. However, FITARA has generally limited application to the Department of Defense.

[14] Major IT investment means a system or an acquisition requiring special management attention because it has significant program or policy implications; high executive visibility; high development, operating, or maintenance costs; an unusual funding mechanism; or is defined as major by the agency's capital planning and investment control process.

conduct a review aimed at identifying and addressing the causes of the risk.

- **Agency CIO authority enhancements.** Agency heads at covered agencies are required to ensure that CIOs have authority to (1) approve the IT budget requests of their respective agencies, (2) certify that OMB's incremental development guidance is being adequately implemented for IT investments, (3) review and approve contracts for IT, and (4) approve the appointment of other agency employees with the title of CIO.
- **Portfolio review.** Covered agencies are to annually review IT investment portfolios in order to, among other things, increase efficiency and effectiveness and identify potential waste and duplication. In establishing the process associated with such portfolio reviews, the law requires OMB to develop standardized performance metrics, to include cost savings, and to submit quarterly reports to Congress on cost savings.
- **Expansion of training and use of IT acquisition cadres.** Covered agencies are to update their acquisition human capital plans to address supporting the timely and effective acquisition of IT. In doing so, the law calls for agencies to consider, among other things, establishing IT acquisition cadres or developing agreements with other agencies that have such cadres.
- **Government-wide software purchasing program.** The General Services Administration is to develop a strategic sourcing initiative to enhance government-wide acquisition and management of software. In doing so, the law requires that, to the maximum extent practicable, the General Services Administration should allow for the purchase of a software license agreement that is available for use by all executive branch agencies as a single user.[15]
- **Maximizing the benefit of the Federal Strategic Sourcing Initiative.**[16] Federal agencies are required to compare their

[15] The Making Electronic Government Accountable by Yielding Tangible Efficiencies Act of 2016, or the "MEGABYTE Act" further enhances CIOs' management of software licenses by requiring agency CIOs to establish an agency software licensing policy and a comprehensive software license inventory to track and maintain licenses, among other requirements. Pub. L. No. 114-210 (July 29, 2016); 130 Stat. 824.

[16] The Federal Strategic Sourcing Initiative is a program established by the General Services Administration and the Department of the Treasury to address government-wide opportunities to strategically source commonly purchased goods and services and eliminate duplication of efforts across agencies.

purchases of services and supplies to what is offered under the Federal Strategic Sourcing Initiative. The Administrator for Federal Procurement Policy was also required to issue regulations related to the initiative.

In June 2015, OMB released guidance describing how agencies are to implement FITARA.[17] This guidance is intended to, among other things:

- assist agencies in aligning their IT resources with statutory requirements;
- establish government-wide IT management controls that will meet the law's requirements, while providing agencies with flexibility to adapt to unique agency processes and requirements;
- strengthen the relationship between agency CIOs and bureau CIOs; and
- strengthen CIO accountability for IT costs, schedules, performance, and security.

The guidance identified several actions that agencies were to take to establish a basic set of roles and responsibilities (referred to as the common baseline) for CIOs and other senior agency officials, which were needed to implement the authorities described in the law. For example, agencies were required to conduct a self-assessment and submit a plan describing the changes they intended to make to ensure that common baseline responsibilities were implemented. Agencies were to submit their plans to OMB's Office of E-Government and Information Technology by August 15, 2015, and make portions of the plans publicly available on agency websites no later than 30 days after OMB approval. As of November 2016, all agencies had made their plans publicly available.

In addition, in August 2016, OMB released guidance intended to, among other things, define a framework for achieving the data center consolidation and optimization requirements of FITARA.[18] The guidance requires each agency on a quarterly basis to:

[17] OMB, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).

[18] OMB, *Data Center Optimization Initiative (DCOI)*, Memorandum M-16-19 (Washington D.C.: Aug. 1, 2016).

- maintain complete inventories of all data center facilities owned, operated, or maintained by or on behalf of the agency;
- develop cost savings targets for fiscal years 2016 through 2018 and report any actual realized cost savings; and
- measure progress toward meeting optimization metrics.

The guidance also directs agencies to develop a data center consolidation and optimization strategic plan that defines the agency's data center strategy for fiscal years 2016, 2017, and 2018. This strategy is to include, among other things, a statement from the agency CIO indicating whether the agency has complied with all data center reporting requirements in FITARA. Further, the guidance indicates that OMB is to maintain a public dashboard that will display consolidation-related costs savings and optimization performance information for the agencies.

IT Acquisitions and Operations Identified by GAO as a High-Risk Area

In February 2015, we introduced a new government-wide high-risk area, *Improving the Management of IT Acquisitions and Operations.*[19] This area highlighted several critical IT initiatives in need of additional congressional oversight, including (1) reviews of troubled projects; (2) efforts to increase the use of incremental development; (3) efforts to provide transparency relative to the cost, schedule, and risk levels for major IT investments; (4) reviews of agencies' operational investments; (5) data center consolidation; and (6) efforts to streamline agencies' portfolios of IT investments. We noted that implementation of these initiatives was inconsistent and more work remained to demonstrate progress in achieving IT acquisition and operation outcomes.

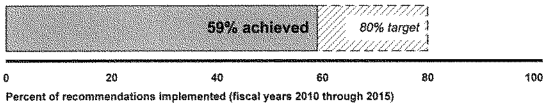
Further, our February 2015 high-risk report stated that, beyond implementing FITARA, OMB and agencies needed to continue to implement our prior recommendations in order to improve their ability to effectively and efficiently invest in IT. Specifically, from fiscal years 2010 through 2015, we made 803 recommendations to OMB and federal agencies to address shortcomings in IT acquisitions and operations. These recommendations included many to improve the implementation of the aforementioned six critical IT initiatives and other government-wide, cross-cutting efforts. We stressed that OMB and agencies should demonstrate government-wide progress in the management of IT investments by, among other things, implementing at least 80 percent of

[19] GAO-15-290.

our recommendations related to managing IT acquisitions and operations within 4 years.

In February 2017, we issued an update to our high-risk series and reported that, while progress had been made in improving the management of IT acquisitions and operations, significant work still remained to be completed.[20] For example, as of March 2018, OMB and agencies had fully implemented 476 (or about 59 percent) of the 803 recommendations. Figure 1 summarizes the progress that OMB and agencies have made in addressing our recommendations as compared to the 80 percent target, as of March 2018.

Figure 1: Summary of the Office of Management and Budget's and Federal Agencies' Progress in Addressing GAO's Recommendations, as of March 2018



Source: Office of Management and Budget and agency data. | GAO-18-460T

In addition, in fiscal year 2016, we made 202 new recommendations, thus further reinforcing the need for OMB and agencies to address the shortcomings in IT acquisitions and operations. Also, beyond addressing our prior recommendations, our 2017 high-risk update noted the importance of OMB and covered federal agencies continuing to expeditiously implement the requirements of FITARA.

To further explore the challenges and opportunities to improve federal IT acquisitions and operations, we convened a forum on September 14, 2016, to explore challenges and opportunities for CIOs to improve federal IT acquisitions and operations—with the goal of better informing policymakers and government leadership.[21] Forum participants, which included 13 current and former federal agency CIOs, members of Congress, and private sector IT executives, identified key actions related to seven topics: (1) strengthening FITARA, (2) improving CIO authorities,

[20] GAO-17-317.

[21] GAO, *Information Technology: Opportunities for Improving Acquisitions and Operations,* GAO-17-251SP (Washington, D.C.: Apr. 11, 2017).

(3) budget formulation, (4) governance, (5) workforce, (6) operations, and (7) transition planning. A summary of the key actions, by topic area, identified during the forum is provided in figure 2.

Figure 2: Key Actions, by Topic Area, Identified by Forum Participants to Improve Information Technology Acquisitions and Operations

STRENGTHENING FITARA'S IMPACT	• Congressional oversight could be more aggressive • Office of Management and Budget (OMB) may need to strengthen its role • The Department of Defense should be required to implement all provisions of the Federal Information Technology Acquisition Reform Act (FITARA)
IMPROVING CIO AUTHORITIES	• Have the Chief Information Officers (CIO) Council play an enhanced role in improving authorities • Implement collaborative governance • Evolve the role of the CIO to enable change • Focus on cybersecurity to change existing cultures
BUDGET FORMULATION	• Use information technology (IT) spend plans to improve budgets • Examine agency programs to capture additional IT spending • Simplify the definition of IT • Work more closely with procurement organizations • Work with congressional committees to explore budgeting flexibilities
GOVERNANCE	• Obtain support from agency leadership • Enhance governance at OMB and agencies • Use security authorities to enhance governance • Strengthen oversight for IT purchased as a service • Buy more and develop less • Evolve procurement processes to align with new technologies
WORKFORCE	• Attract more qualified CIOs by appealing to key missions • Have the Federal CIO play a more active role in attracting agency CIOs • Give CIOs more human resource flexibilities • Focus on attracting and investing in a more holistic IT workforce • Better integrate private sector talent into the IT workforce
OPERATIONS	• Use a strategic approach for legacy system migration • Migrate more services to the cloud • Implement strategies to mitigate the impact on jobs when closing data centers
TRANSITION PLANNING	• Convey IT and cyber issues early to leadership • Encourage Congress to focus on IT and cybersecurity at confirmation hearings • Ensure that IT and cyber issues are OMB priorities • Ensure GAO plays a role highlighting its work and expertise

Source: GAO analysis. | GAO-18-460T

In addition, in January 2017, the Federal CIO Council concluded that differing levels of authority over IT-related investments and spending have led to inconsistencies in how IT is executed from agency to agency. According to the Council, for those agencies where the CIO has broad authority to manage all IT investments, great progress has been made to streamline and modernize the federal agency's footprint. For the others, where agency CIOs are only able to control pieces of the total IT footprint, it has been harder to achieve improvements.[22]

Congress Has Taken Action to Continue Selected FITARA Provisions and Modernize Federal IT

Congress has recognized the importance of covered agencies' continued implementation of FITARA provisions, and has taken legislative action to extend selected provisions beyond their original dates of expiration. Specifically, Congress and the President enacted laws to:[23]

- remove the expiration date for enhanced transparency and improved risk management provisions, which were set to expire in 2019;
- remove the expiration date for portfolio review, which was set to expire in 2019;
- extend the expiration date for FDCCI from 2018 to 2020; and
- authorize the availability of funding mechanisms to help further agencies' efforts to modernize IT.[24]

In particular, a law was enacted to authorize the availability of funding to help further agencies' efforts to modernize IT. The law, known as the Modernizing Government Technology (MGT) Act, authorizes agencies to establish working capital funds for use in transitioning from legacy IT systems, as well as for addressing evolving threats to information security. The law creates a technology modernization fund within the Department of the Treasury, from which agencies can "borrow" money to retire and replace legacy systems as well as acquire or develop systems.

The Current Administration Has Undertaken Efforts to Improve Federal IT

The current administration has initiated additional efforts aimed at improving federal IT, including digital services. Specifically, in March 2017, the administration established the Office of American Innovation, which has a mission to, among other things, make recommendations to the President on policies and plans aimed at improving federal

[22] CIO Council, *State of Federal Information Technology* (Washington, D.C.: January 2017).

[23] *FITARA Enhancement Act of 2017*, Pub. L. No. 115-88, 131 Stat. 1278 (2017).

[24] *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91,Div. A, Title X, Subtitle G (2017).

government operations and services. In doing so, the office is to consult with both OMB and the Office of Science and Technology Policy on policies and plans intended to improve government operations and services, improve the quality of life for Americans, and spur job creation.[25]

In May 2017, the administration also established the American Technology Council, which has a goal of helping to transform and modernize federal agency IT and how the federal government uses and delivers digital services.[26] The President is the chairman of this council, and the Federal CIO and the United States Digital Service[27] Administrator are among the members.

In addition, on May 11, 2017, the President signed Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*[28] This Executive Order tasked the Director of American Technology Council[29] to coordinate a report to the President from the Secretary of the Department of Homeland Security, the Director of OMB, and the Administrator of the General Services Administration, in consultation with the Secretary of Commerce, regarding the modernization of federal IT. As a result, the *Report to the President on Federal IT Modernization* was issued on December 13, 2017, and outlined the current and envisioned state of federal IT. The report recognized that agencies have attempted to modernize systems but have been stymied by a variety of factors, including resource prioritization, ability to procure services quickly, and technical issues. The report provided multiple recommendations intended to address these issues through the modernization and consolidation of networks and the use of shared services to enable future network architectures.

[25] The White House Office of Science and Technology Policy provides the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics.

[26] Exec. Order No. 13794, Establishment of the American Technology Council, 82 Fed. Reg. 20811 (Mary 3, 2017).

[27] The United States Digital Service is an office within OMB which aims to improve the most important public-facing federal digital services.

[28] Exec. Order No. 13800, 82 Fed Reg. 22391 (May 16, 2017).

[29] An employee of the Executive Office of the President designated by the President.

In February 2018, OMB issued guidance[30] for agencies to implement the MGT Act. The guidance was intended to provide agencies additional information regarding the Technology Management Fund, and the administration and funding of the related IT Working Capital Funds. Specifically, the guidance allowed agencies to begin submitting initial project proposals for modernization on February 27, 2018. In addition, in accord with the MGT Act, the guidance provides details of the Technology Modernization Board, which is to consist of (1) the Federal CIO; (2) a senior official from the General Services Administration; (3) a member of the Department of Homeland Security's National Protection and Program Directorate; and (4) four federal employees with technical expertise in IT development, financial management, cyber security and privacy, and acquisition, appointed by the Director of OMB.

Agencies Can Improve IT Acquisitions and Operations

Agencies have taken steps to improve the management of IT acquisitions and operations. However, agencies would be better positioned to realize billions in cost savings and additional management improvements, if they addressed the numerous recommendations we have made aimed at improving data center consolidation, increasing transparency via OMB's IT Dashboard, implementing incremental development, managing software licenses, reviewing IT acquisitions, implementing key IT workforce activities, and addressing aging legacy systems.

Agencies Have Made Progress in Consolidating Data Centers, but Need to Take Action to Achieve Planned Cost Savings

One of the key initiatives to implement FITARA is data center consolidation. OMB established FDCCI in February 2010 to improve the efficiency, performance, and environmental footprint of federal data center activities, and the enactment of FITARA codified and expanded the initiative. However, in a series of reports that we issued from July 2011 through August 2017, we noted that, while data center consolidation could potentially save the federal government billions of dollars, weaknesses existed in several areas, including agencies' data center consolidation plans, data center optimization, and OMB's tracking and

[30] Office of Management and Budget, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

reporting on related cost savings.[31] In these reports, we made a matter for Congressional consideration, and a total of 160 recommendations to OMB and 24 agencies to improve the execution and oversight of the initiative. Most agencies and OMB agreed with our recommendations or had no comments. As of March 2018, 83 of these recommendations remained open.

For example, in May 2017, we reported[32] that the 24 agencies[33] participating in FDCCI collectively had made progress on their data center closure efforts. Specifically, as of August 2016, these agencies had identified a total of 9,995 data centers, of which they reported having closed 4,388, and having plans to close a total of 5,597 data centers through fiscal year 2019. Notably, the Departments of Agriculture, Defense, the Interior, and the Treasury accounted for 84 percent of the completed closures.

In addition, that report noted that 18 of the 24 agencies had reported achieving about $2.3 billion collectively in cost savings and avoidances from their data center consolidation and optimization efforts from fiscal year 2012 through August 2016. The Departments of Commerce,

[31] GAO, *Data Center Optimization: Agencies Need to Address Challenges and Improve Progress to Achieve Cost Savings Goal,* GAO-17-448 (Washington, D.C.: Aug. 15, 2017); *Data Center Optimization: Agencies Need to Complete Plans to Address Inconsistencies in Reported Savings*, GAO-17-388 (Washington, D.C.: May 18, 2017); *Data Center Consolidation: Agencies Making Progress, but Planned Savings Goals Need to Be Established [Reissued on March 4, 2016],* GAO-16-323 (Washington, D.C.: Mar. 3, 2016); *Data Center Consolidation: Reporting Can Be Improved to Reflect Substantial Planned Savings,* GAO-14-713 (Washington, D.C.: Sept. 25, 2014); *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal,* GAO-13-378 (Washington, D.C.: Apr. 23, 2013); *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed,* GAO-12-742 (Washington, D.C.: July 19, 2012); and *Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings,* GAO-11-565 (Washington, D.C.: July 19, 2011).

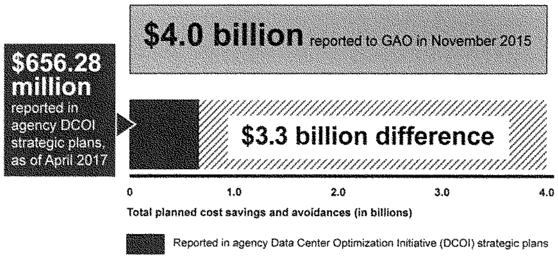
[32] GAO-17-388.

[33] The 24 agencies that FITARA requires to participate in FDCCI are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

Defense, Homeland Security, and the Treasury accounted for approximately $2.0 billion (or 87 percent) of the total.

Further, 23 agencies reported about $656 million collectively in planned savings for fiscal years 2016 through 2018. This is about $3.3 billion less than the estimated $4.0 billion in planned savings for fiscal years 2016 through 2018 that agencies reported to us in November 2015. Figure 3 presents a comparison of the amounts of cost savings and avoidances reported by agencies to OMB and the amounts the agencies reported to us.

Figure 3: Comparison of Fiscal Years 2016-2018 Planned Cost Savings and Avoidances Reported to GAO in November 2015 versus Those Reported to the Office of Management and Budget in April 2017



Source: GAO analysis of agency data. | GAO-18-460T

As mentioned previously, FITARA required agencies to submit no later than the end of fiscal year 2016 and annually thereafter multi-year strategies to achieve the consolidation and optimization of their data centers. Among other things, this strategy is required to include such information as data center consolidation and optimization metrics, and year-by-year calculations of investments and cost savings through October 1, 2020.

Further, OMB's August 2016 guidance on data center optimization contained additional information for how agencies are to implement the strategic plan requirements of FITARA, and stated that agencies were required to publicly post their strategic plans to their agency-owned digital strategy websites by September 30, 2016.[34]

As of April 2017, only 7 of the 23 agencies that submitted their strategic plans—the Departments of Agriculture, Education, Homeland Security, and Housing and Urban Development; the General Services Administration; the National Science Foundation; and the Office of Personnel Management—had addressed all five elements required by the OMB memorandum implementing FITARA. The remaining 16 agencies either partially met or did not meet the requirements. For example, most agencies partially met or did not meet the requirements to provide information related to data center closures and cost savings metrics. The Department of Defense did not submit a plan and was rated as not meeting any of the requirements.

To better ensure that federal data center consolidation and optimization efforts improve governmental efficiency and achieve cost savings, in our May 2017 report, we recommended that 11 of the 24 agencies take actions to ensure that the amounts of achieved data center cost savings and avoidances are consistent across all reporting mechanisms. We also recommended that 17 of the 24 agencies each take action to complete missing elements in their strategic plans and submit their plans to OMB in order to optimize their data centers and achieve cost savings. Twelve agencies agreed with our recommendations, 2 did not agree, and 10 agencies and OMB did not state whether they agreed or disagreed.

More recently, in August 2017, we reported that agencies needed to address challenges in optimizing their data centers in order to achieve cost savings.[35] Specifically, we noted that, according to the 24 agencies' data center consolidation initiative strategic plans as of April 2017, most agencies were not planning to meet OMB's optimization targets by the end of fiscal year 2018. Further, of the 24 agencies, 5—the Department of Commerce and the Environmental Protection Agency, National Science Foundation, Small Business Administration, and U.S. Agency for International Development—reported plans to fully meet their applicable

[34] OMB, *Data Center Optimization Initiative (DCOI)*, Memorandum M-16-19 (Washington, D.C.: Aug. 1, 2016).

[35] GAO-17-448.

targets by the end of fiscal year 2018;[36] 13 reported plans to meet some, but not all, of the targets; 4 reported that they did not plan to meet any targets; and 2 did not have a basis to report planned optimization milestones because they do not report having any agency-owned data centers. Figure 4 summarizes agencies' progress in meeting OMB's optimization targets as of February 2017, and planned progress to be achieved by September 2017 and September 2018, as of April 2017.

[36] U.S. Agency for International Development did not have any tiered data centers in its data center inventory. Therefore, the agency only had a basis to report on its plans to meet the one OMB optimization metric applicable to its non-tiered data centers (i.e., server utilization and automated monitoring).

Figure 4: Agency-Reported Plans to Meet or Exceed the Office of Management and Budget's (OMB) Data Center Optimization Targets

Agency	Current progress from OMB's Information Technology Dashboard (as of February 2017)	Planned optimization performance from agency data center optimization strategic plan (as of April 2017)	
		September 2017	September 2018
Department of Agriculture	▨□□□□	▨□□□□	▨□□□□
Department of Commerce	□□□□□	▨▨▨□□	▨▨▨▨▨
Department of Defense	□□□□□	□□□□□	□□□□□
Department of Education[a]	Not applicable	Not applicable	Not applicable
Department of Energy	□□□□□	□□□□□	▨▨▨▨□
Department of Health and Human Services	▨□□□□	▨□□□□	▨□□□□
Department of Homeland Security	□□□□□	□□□□□	□□□□□
Department of Housing and Urban Development[a]	Not applicable	Not applicable	Not applicable
Department of the Interior	□□□□□	□□□□□	□□□□□
Department of Justice	□□□□□	□□□□□	▨□□□□
Department of Labor	□□□□□	□□□□□	▨▨▨▨□
Department of State	▨□□□□	▨▨□□□	▨▨□□□
Department of Transportation	□□□□□	□□□□□	□□□□□
Department of the Treasury	□□□□□	▨□□□□	▨▨□□□
Department of Veterans Affairs	▨□□□□	□□□□□	▨▨▨□□
Environmental Protection Agency	▨▨▨□□	▨▨□□□	▨▨▨▨▨
General Services Administration	▨□□□□	▨□□□□	▨□□□□
National Aeronautics and Space Administration	□□□□□	□□□□□	▨□□□□
National Science Foundation[b]	□	▨▨▨□□	▨▨▨▨▨
Nuclear Regulatory Commission	▨□□□□	▨□□□□	▨□□□□
Office of Personnel Management	▨□□□□	▨□□□□	▨▨▨□□
Small Business Administration	□□□□□	▨□□□□	▨▨▨▨▨
Social Security Administration	▨▨▨□□	▨▨▨□□	▨▨▨□□
U.S. Agency for International Development[c]	□	□	▨

Source: GAO analysis of OMB Information Technology Dashboard and agency data. | GAO-18-460T

Note: The five boxes in each column represent OMB's five optimization targets relative to (1) server utilization and automated monitoring; (2) energy metering; (3) power usage effectiveness; (4) facility utilization; and (5) virtualization. The shaded areas identify agencies' current and planned progress in meeting or exceeding OMB's fiscal year 2018 target for each metric.

[a]Agency did not have any reported agency-owned data centers in its inventory and, therefore, did not have a basis to measure and report on optimization progress.

[b]The National Science Foundation did not have any reported agency-owned tiered data centers in its inventory as of February 2017 and, therefore, did not have a basis to report on progress for four of the five metrics. However, according to the agency's April 2017 data center optimization strategic plan, it will have a basis to report on all five metrics in fiscal years 2017 and 2018.

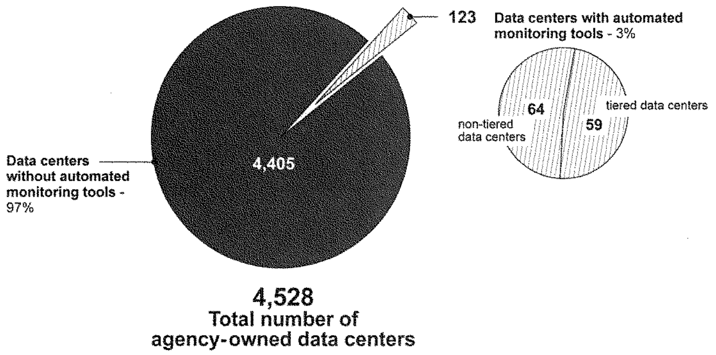
[c]The U.S. Agency for International Development did not have any reported agency-owned tiered data centers in its inventory and, therefore, did not have a basis to measure and report on four of the five metrics.

FITARA required OMB to establish a data center optimization metric specific to measuring server efficiency, and required agencies to report on progress in meeting this metric. To effectively measure progress against this metric, OMB directed agencies to replace the manual collection and reporting of systems, software, and hardware inventory housed within agency-owned data centers with automated monitoring tools and to complete this effort no later than the end of fiscal year 2018. Agencies are required to report progress in implementing automated monitoring tools and server utilization averages at each data center as part of their quarterly data center inventory reporting to OMB.

As of February 2017, 4 of the 22 agencies reporting agency-owned data centers in their inventory[37]—the National Aeronautics and Space Administration, National Science Foundation, Social Security Administration, and U.S. Agency for International Development—reported that they had implemented automated monitoring tools at all of their data centers. Further, 10 reported that they had implemented automated monitoring tools at between 1 and 57 percent of their centers, and 8 had not yet begun to report the implementation of these tools. In total, the 22 agencies reported that automated tools were implemented at 123 (or about 3 percent) of the 4,528 total agency-owned data centers, while the remaining 4,405 (or about 97 percent) of these data centers were not reported as having these tools implemented. Figure 5 summarizes the number of agency-reported data centers with automated monitoring tools implemented, including the number of tiered and non-tiered centers.

[37]Two agencies—the Department of Education and Housing and Urban Development—do not have any agency-owned data centers; therefore, they do not have a basis for implementing automated monitoring tools.

Figure 5: Number of Agency-Reported Data Centers with Automated Monitoring Tools Implemented, as of February 2017



Source: GAO analysis of Office of Management and Budget and agency data. | GAO-18-460T

To address challenges in optimizing federal data centers, in our August 2017 report, we made recommendations to 18 agencies and OMB. Ten agencies agreed with our recommendations, three agencies partially agreed, and six (including OMB) did not state whether they agreed or disagreed.

Risks Need to Be Fully Considered When Agencies Rate Their Major Investments on OMB's IT Dashboard

To facilitate transparency across the government in acquiring and managing IT investments, OMB established a public website—the IT Dashboard—to provide detailed information on major investments at 26 agencies, including ratings of their performance against cost and schedule targets. Among other things, agencies are to submit ratings from their CIOs, which, according to OMB's instructions, should reflect the level of risk facing an investment relative to that investment's ability to accomplish its goals. In this regard, FITARA includes a requirement for covered agency CIOs to categorize their major IT investment risks in accordance with OMB guidance.[38]

[38] 40 U.S.C. § 11302(c)(3)(C).

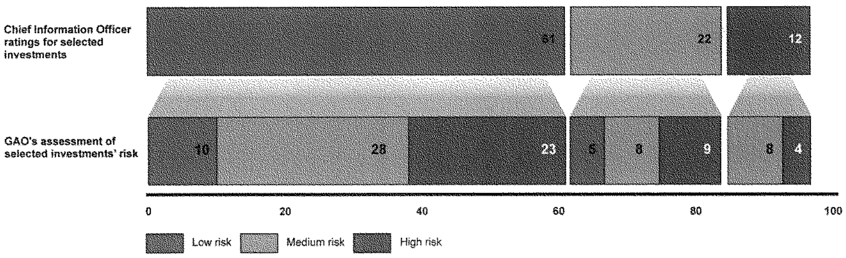
Over the past 6 years, we have issued a series of reports about the Dashboard that noted both significant steps OMB has taken to enhance the oversight, transparency, and accountability of federal IT investments by creating its Dashboard, as well as concerns about the accuracy and reliability of the data.[39] In total, we have made 47 recommendations to OMB and federal agencies to help improve the accuracy and reliability of the information on the Dashboard and to increase its availability. Most agencies agreed with our recommendations or had no comments. As of March 2018, 19 recommendations remained open.

In June 2016, we determined that 13 of the 15 agencies selected for in-depth review had not fully considered risks when rating their major investments on the Dashboard. Specifically, our assessments of risk for 95 investments at the 15 selected agencies[40] matched the CIO ratings posted on the Dashboard 22 times, showed more risk 60 times, and showed less risk 13 times. Figure 6 summarizes how our assessments compared to the selected investments' CIO ratings.

[39] GAO, *IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments,* GAO-16-494 (Washington, D.C.: June 2, 2016); *IT Dashboard: Agencies Are Managing Investment Risk, but Related Ratings Need to Be More Accurate and Available,* GAO-14-64 (Washington, D.C.: Dec. 12, 2013); *IT Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies,* GAO-13-98 (Washington, D.C.: Oct. 16, 2012); *IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making,* GAO-12-210 (Washington, D.C.: Nov. 7, 2011); *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy,* GAO-11-262 (Washington, D.C.: Mar. 15, 2011); and *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed,* GAO-10-701 (Washington, D.C.: July 16, 2010).

[40] The 15 selected agencies were the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, the Interior, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; and Social Security Administration.

Figure 6: Comparison of Selected Investments' April 2015 Chief Information Officer Ratings to GAO's Assessments



Source: GAO's assessment of data from the Office of Management and Budget's Information Technology Dashboard. | GAO-18-460T

Aside from the inherently judgmental nature of risk ratings, we identified three factors which contributed to differences between our assessments and the CIO ratings:

- Forty of the 95 CIO ratings were not updated during April 2015 (the month we conducted our review), which led to differences between our assessments and the CIOs' ratings. This underscores the importance of frequent rating updates, which help to ensure that the information on the Dashboard is timely and accurately reflects recent changes to investment status.
- Three agencies' rating processes spanned longer than 1 month. Longer processes mean that CIO ratings are based on older data, and may not reflect the current level of investment risk.
- Seven agencies' rating processes did not focus on active risks. According to OMB's guidance, CIO ratings should reflect the CIO's assessment of the risk and the investment's ability to accomplish its goals. CIO ratings that do no incorporate active risks increase the chance that ratings overstate the likelihood of investment success.

As a result, we concluded that the associated risk rating processes used by the 15 agencies were generally understating the level of an investment's risk, raising the likelihood that critical federal investments in IT are not receiving the appropriate levels of oversight.

To better ensure that the Dashboard ratings more accurately reflect risk, we made 25 recommendations to 15 agencies to improve the quality and frequency of their CIO ratings. Twelve agencies generally agreed with or did not comment on the recommendations and three agencies disagreed, stating that their CIO ratings were adequate. However, we noted that weaknesses in these three agencies' processes still existed and that we continued to believe our recommendations were appropriate.

Agencies Need to Increase Their Use of Incremental Development Practices

OMB has emphasized the need to deliver investments in smaller parts, or increments, in order to reduce risk, deliver capabilities more quickly, and facilitate the adoption of emerging technologies. In 2010, it called for agencies' major investments to deliver functionality every 12 months and, since 2012, every 6 months. Subsequently, FITARA codified a requirement that covered agency CIOs certify that IT investments are adequately implementing incremental development, as defined in the capital planning guidance issued by OMB.[41] Further, subsequent OMB guidance on the law's implementation, issued in June 2015, directed agency CIOs to define processes and policies for their agencies which ensure that they certify that IT resources are adequately implementing incremental development.[42]

However, in May 2014, we reported[43] that 66 of 89 selected investments at five major agencies[44] did not plan to deliver capabilities in 6-month cycles, and less than half of these investments planned to deliver functionality in 12-month cycles. We also reported that only one of the five agencies had complete incremental development policies. Accordingly, we recommended that OMB clarify its guidance on incremental development and that the selected agencies update their associated policies to comply with OMB's revised guidance (once made available), and consider the factors identified in our report when doing so.

Four of the six agencies agreed with our recommendations or had no comments, one agency partially agreed, and the remaining agency disagreed with the recommendations. The agency that disagreed did not believe that its recommendations should be dependent upon OMB taking

[41] 40 U.S.C. § 11319(b)(1)(B)(ii).

[42] OMB, Memorandum M-15-14.

[43] GAO, *Information Technology: Agencies Need to Establish and Implement Incremental Development Policies*, GAO-14-361 (Washington, D.C.: May 1, 2014).

[44] These five agencies are the Departments of Defense, Health and Human Services, Homeland Security, Transportation, and Veterans Affairs.

action to update guidance. In response, we noted that only one of the recommendations to that agency depended upon OMB action, and we maintained that the action was warranted and could be implemented.

Subsequently, in August 2016, we reported[45] that agencies had not fully implemented incremental development practices for their software development projects. Specifically, we noted that, as of August 31, 2015, 22 federal agencies[46] had reported on the Dashboard that 300 of 469 active software development projects (64 percent) were planning to deliver usable functionality every 6 months for fiscal year 2016, as required by OMB guidance. The remaining 169 projects (or 36 percent) that were reported as not planning to deliver functionality every 6 months, agencies provided a variety of explanations for not achieving that goal. These included project complexity, the lack of an established project release schedule, or that the project was not a software development project.

Further, in conducting an in-depth review of seven selected agencies' software development projects,[47] we determined that 129 out of 287 software development projects delivered functionality every 6 months for fiscal year 2015 (45 percent) and 113 out of 206 software projects (55 percent) planned to do so in fiscal year 2016. However, significant differences existed between the delivery rates that the agencies reported to us and what they reported on the Dashboard. For example, for four agencies (the Departments of Commerce, Education, Health and Human Services, and the Treasury), the percentage of delivery reported to us was at least 10 percentage points lower than what was reported on the Dashboard. These differences were due to (1) our identification of fewer software development projects than agencies reported on the Dashboard

[45] GAO, *Information Technology Reform: Agencies Need to Increase Their Use of Incremental Development Practices*, GAO-16-469 (Washington, D.C.: Aug. 16, 2016).

[46] These 22 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Archives and Records Administration, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[47] These seven agencies are the Departments of Commerce, Defense, Education, Health and Human Services, Homeland Security, Transportation, and the Treasury. These agencies were chosen because they reported a minimum of 12 investments that were at least 50 percent or more in development on the Dashboard for fiscal year 2015.

and (2) the fact that information reported to us was generally more current than the information reported on the Dashboard.

We concluded that, by not having up-to-date information on the Dashboard about whether the project is a software development project and about the extent to which projects are delivering functionality, these seven agencies were at risk that OMB and key stakeholders may make decisions regarding the agencies' investments without the most current and accurate information. As such, we recommended that the seven selected agencies review major IT investment project data reported on the Dashboard and update the information as appropriate, ensuring that these data are consistent across all reporting channels.

Finally, while OMB has issued guidance requiring agency CIOs to certify that each major IT investment's plan for the current year adequately implements incremental development, only three agencies (the Departments of Commerce, Homeland Security, and Transportation) had defined processes and policies intended to ensure that the CIOs certify that major IT investments are adequately implementing incremental development.[48] Accordingly, we recommended that the remaining four agencies—the Departments of Defense, Education, Health and Human Services, and the Treasury—establish policies and processes for certifying that major IT investments adequately use incremental development.

The Departments of Education and Health and Human Services agreed with our recommendation, while the Department of Defense disagreed and stated that its existing policies address the use of incremental development. However, we noted that the department's policies did not comply with OMB's guidance and that we continued to believe our recommendation was appropriate. The Department of the Treasury did not comment on its recommendation.

More recently, in November 2017, we reported that agencies needed to improve their certification of incremental development.[49] Specifically, agencies reported that 103 of 166 major IT software development investments (62 percent) were certified by the agency CIO for

[48] Office of Management and Budget, *FY2017 IT Budget – Capital Planning Guidance.*

[49] GAO, *Information Technology Reform: Agencies Need to Improve Certification of Incremental Development,* GAO-18-148 (Washington, D.C.: Nov. 7, 2017).

implementing adequate incremental development in fiscal year 2017, as required by FITARA as of August 2016. Table 1 identifies the number of federal agency major IT software development investments certified for adequate incremental development, as reported on the IT Dashboard for fiscal year 2017.

Table 1: Federal Agency Major Information Technology (IT) Software Development Investments Certified for Adequate Incremental Development, as Reported on the IT Dashboard for Fiscal Year 2017

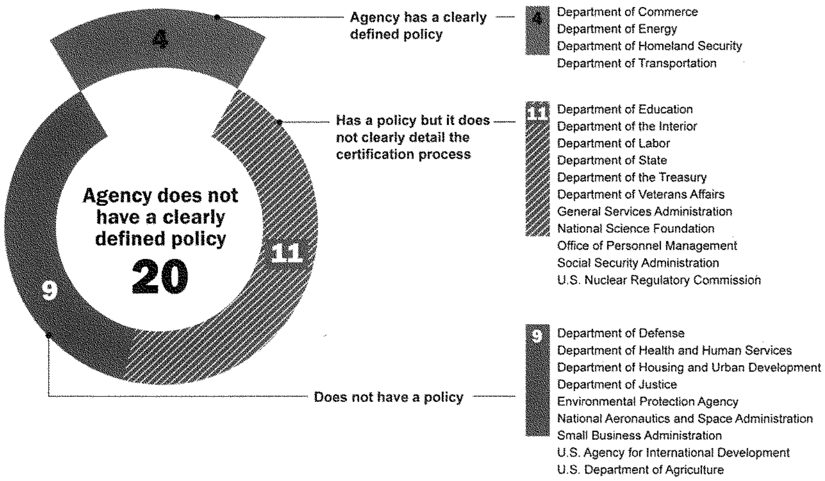
Agency	Number of major investments	Number of investments certified for adequate incremental development	Percent of investments certified for adequate incremental development
U.S. Department of Agriculture	7	4	57%
Department of Commerce	11	10	91%
Department of Defense	33	10	30%
Department of Education	7	6	86%
Department of Energy	3	1	33%
Department of Health and Human Services	24	20	83%
Department of Homeland Security	10	6	60%
Department of Housing and Urban Development	1	1	100%
Department of the Interior	6	4	67%
Department of Justice	2	2	100%
Department of Labor	1	1	100%
Department of State	5	5	100%
Department of Transportation	12	3	25%
Department of the Treasury	10	3	30%
Department of Veterans Affairs	10	10	100%
Environmental Protection Agency	1	1	100%
General Services Administration	7	7	100%
Office of Personnel Management	3	3	100%
Small Business Administration	2	2	100%
Social Security Administration	10	3	30%
U.S. Agency for International Development	1	1	100%
Total	**166**	**103**	**62%**

Source: GAO analysis of IT Dashboard data as of August 31, 2016. | GAO-18-460T

Officials from 21 of the 24 agencies in our review reported that challenges hindered their ability to implement incremental development, which included: (1) inefficient governance processes; (2) procurement delays; and (3) organizational changes associated with transitioning from a traditional software methodology that takes years to deliver a product, to incremental development, which delivers products in shorter time frames. Nevertheless, 21 agencies reported that the certification process was beneficial because they used the information from the process to assist with identifying investments that could more effectively use an incremental approach, and used lessons learned to improve the agencies' incremental processes.

In addition, as of August 2017, only 4 of the 24 agencies had clearly defined CIO incremental development certification policies and processes that contained descriptions of the role of the CIO in the process and how the CIO's certification will be documented; and included definitions of incremental development and time frames for delivering functionality consistent with OMB guidance. Figure 7 summarizes our analysis of agencies' policies for CIO certification of the adequate use of incremental development in IT investments.

Figure 7: Analysis of Agencies' Policies for Chief Information Officer Certification of the Adequate Use of Incremental Development in Information Technology Investments



Source: GAO analysis of agency Chief Information Officer certification policies and processes. | GAO-18-460T

Lastly, we reported that OMB's capital planning guidance for fiscal year 2018[50] (issued in June 2016) lacked clarity regarding how agencies were to address the requirement for certifying adequate incremental development. While the 2018 guidance stated that agency CIOs are to provide the certifications needed to demonstrate compliance with FITARA, the guidance did not include a specific reference to the provision requiring CIO certification of adequate incremental development. We noted that, as a result of this change, OMB placed the burden on agencies to know and understand how to demonstrate compliance with FITARA's incremental development provision. Further, because of the lack of clarity in the guidance as to what agencies were to provide, OMB

[50] OMB, FY 2017 IT Budget–Capital Planning Guidance.

could not demonstrate how the fiscal year 2018 guidance ensured that agencies provided the certifications specifically called for in the law.

In August 2017, OMB issued its fiscal year 2019 guidance,[51] which addressed the weaknesses we identified in the previous fiscal year's guidance. Specifically, the revised guidance requires agency CIOs to make an explicit statement regarding the extent to which the CIO is able to certify the use of incremental development, and to include a copy of that statement in the agency's public congressional budget justification materials. As part of the statement, an agency CIO must also identify which specific bureaus or offices are using incremental development on all of their investments.

In our November 2017 report, we made 19 recommendations to 17 agencies to improve reporting and certification of incremental development. Eleven agencies agreed with our recommendations, 1 partially agreed, and 5 did not state whether they agreed or disagreed. OMB disagreed with several of our conclusions, which we continued to believe were valid.

In total, from May 2014 through November 2017, we made 42 recommendations to OMB and agencies to improve their implementation of incremental development. As of March 2018, 34 of our recommendations remained open.

Agencies Need to Better Manage Software Licenses to Achieve Savings

Federal agencies engage in thousands of software licensing agreements annually. The objective of software license management is to manage, control, and protect an organization's software assets. Effective management of these licenses can help avoid purchasing too many licenses, which can result in unused software, as well as too few licenses, which can result in noncompliance with license terms and cause the imposition of additional fees.

As part of its PortfolioStat initiative, OMB has developed policy that addresses software licenses. This policy requires agencies to conduct an annual, agency-wide IT portfolio review to, among other things, reduce commodity IT spending. Such areas of spending could include software licenses.

[51] OMB, FY 2019 IT Budget–Capital Planning Guidance.

In May 2014, we reported on federal agencies' management of software licenses and determined that better management was needed to achieve significant savings government-wide.[52] In particular, 22 of the 24 major agencies did not have comprehensive license policies and only 2 had comprehensive license inventories. In addition, we identified five leading software license management practices, and the agencies' implementation of these practices varied.

As a result of agencies' mixed management of software licensing, agencies' oversight of software license spending was limited or lacking, thus potentially leading to missed savings. However, the potential savings could be significant considering that, in fiscal year 2012, 1 major federal agency reported saving approximately $181 million by consolidating its enterprise license agreements, even when its oversight process was ad hoc. Accordingly, we recommended that OMB issue needed guidance to agencies; we also made 135 recommendations to the 24 agencies to improve their policies and practices for managing licenses. Among other things, we recommended that the agencies regularly track and maintain a comprehensive inventory of software licenses and analyze the inventory to identify opportunities to reduce costs and better inform investment decision making.

Most agencies generally agreed with the recommendations or had no comments. As of March 2018, 95 of the recommendations had not been implemented. Table 2 reflects the extent to which agencies implemented recommendations in these areas.

Table 2: Agencies' Implementation of Software License Management Recommendations

Agency	Tracks and maintains a comprehensive inventory	Uses inventory to make decisions and reduce costs
Department of Agriculture	●	●
Department of Commerce	◐	●
Department of Defense	◐	◐
Department of Education	●	●
Department of Energy	◐	◐

[52] GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide,* GAO-14-413 (Washington, D.C.: May 22, 2014).

Agency	Tracks and maintains a comprehensive inventory	Uses inventory to make decisions and reduce costs
Department of Health and Human Services	◐	◐
Department of Homeland Security	◐	◐
Department of Housing and Urban Development	◐	◐
Department of Justice	◐	◐
Department of Labor	●	◐
Department of State	◐	◐
Department of the Interior	◐	◐
Department of the Treasury	◐	◐
Department of Transportation	◐	◐
Department of Veterans Affairs	●	●
Environmental Protection Agency	◐	◐
General Services Administration	●	●
National Aeronautics and Space Administration	●	●
Nuclear Regulatory Commission	◐	◐
National Science Foundation	◐	◐
Office of Personnel Management	◐	◐
Small Business Administration	◐	◐
Social Security Administration	◐	◐
U.S. Agency for International Development	●	●

Key:

● Fully—the agency provided evidence that it fully addressed this recommendation

◐ Partially—the agency had plans to address this recommendation

Source: GAO analysis. | GAO-18-460T

Agencies Need to Ensure That IT Acquisitions Are Reviewed and Approved by Chief Information Officers

FITARA includes a provision to enhance covered agency CIOs' authority through, among other things, requiring agency heads to ensure that CIOs review and approve IT contracts. OMB's FITARA implementation guidance expanded upon this section of FITARA in a number of ways.[53] Specifically, according to the guidance:

- CIOs may review and approve IT acquisition strategies and plans, rather than individual IT contracts;[54]
- CIOs can designate other agency officials to act as their representatives, but the CIOs must retain accountability;[55]
- Chief Acquisition Officers (CAO) are responsible for ensuring that all IT contract actions are consistent with CIO-approved acquisition strategies and plans; and
- CAOs are to indicate to the CIOs when planned acquisition strategies and acquisition plans include IT.

In January 2018, we reported[56] that most of the CIOs at the 22 selected agencies[57] were not adequately involved in reviewing billions of dollars of IT acquisitions. For instance, most of the 22 selected agencies did not identify all of their IT contracts. The selected agencies identified 78,249 IT-related contracts, to which they obligated $14.7 billion in fiscal year 2016. However, we identified 31,493 additional contracts with $4.5 billion obligated, raising the total amount obligated to IT contracts in fiscal year

[53] OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Washington, D.C.: June 10, 2015).

[54] OMB's guidance states that CIOs should only review and approve individual IT contract actions if they are not part of an approved acquisition strategy or plan.

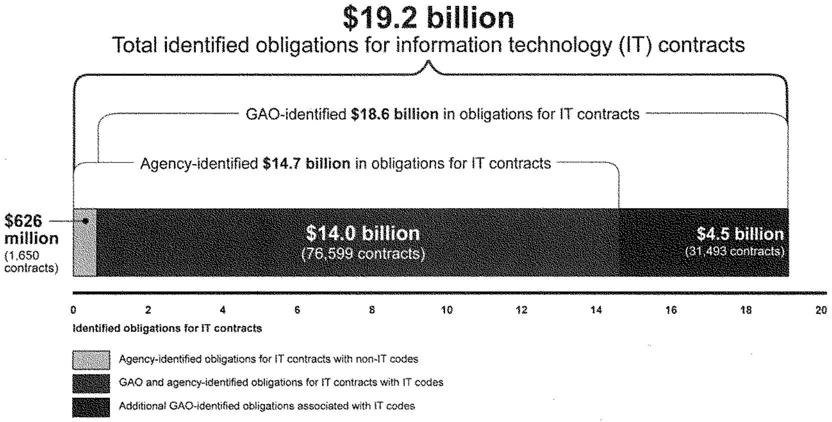
[55] OMB has interpreted FITARA's "governance process" provision to permit such delegation. That provision allows covered agencies to use the governance processes of the agency to approve a contract or other agreement for IT if the CIO of the agency is included as a full participant in the governance process.

[56] GAO, *Information Technology: Agencies Need to Involve Chief Information Officers in Reviewing Billions of Dollars in Acquisitions*, GAO-18-42 (Washington, D.C.: Jan. 10, 2018).

[57] The 22 agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Housing and Urban Development, Justice, Labor, State, the Interior, the Treasury, Transportation, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development.

2016 to at least $19.2 billion. Figure 8 reflects the obligations agencies reported to us relative to the obligations we identified.

Figure 8: Agency- and GAO-Identified Approximate Dollars Obligated to Fiscal Year 2016 IT Contracts at the 22 Selected Agencies



Source: GAO analysis of agency and USAspending.gov data. | GAO-18-460T

The percentage of additional IT contract obligations we identified varied among the selected agencies. For example, the Department of State did not identify 1 percent of its IT contract obligation dollars. Conversely, 8 agencies did not identify over 40 percent of their IT-related contract obligation dollars. Many of the selected agencies that did not identify these IT acquisitions did not follow OMB guidance. Specifically, 14 of the 22 agencies did not involve the acquisition office in their process to identify IT acquisitions for CIO review, as required by OMB. In addition, 7 agencies did not establish guidance to aid officials in recognizing IT. Until agencies involve the acquisitions office in their IT identification processes and establish supporting guidance, they cannot ensure that they will identify all IT acquisitions. Without proper identification of IT acquisitions, agencies and CIOs cannot effectively provide oversight of these acquisitions.

In addition to not identifying all IT contracts, 14 of the 22 selected agencies did not fully satisfy OMB's requirement that the CIO review and approve IT acquisition plans or strategies. Further, only 11 of 96 randomly selected IT contracts at 10 agencies that we evaluated were CIO-reviewed and approved as required by OMB's guidance. The 85 IT contracts not reviewed had a total possible value of approximately $23.8 billion.

Until agencies ensure that CIOs are able to review and approve all IT acquisitions, CIOs will continue to have limited visibility and input into their agencies' planned IT expenditures and will not be able to use the increased authority that FITARA's contract approval provision is intended to provide. Further, agencies will likely miss an opportunity to strengthen CIOs' authority and the oversight of IT acquisitions. As a result, agencies may award IT contracts that are duplicative, wasteful, or poorly conceived.

As a result of this report, we made 39 recommendations, including that agencies ensure that acquisition offices are involved in identifying IT and issue related guidance and ensure that IT acquisitions are reviewed according to OMB guidance. OMB and 20 agencies generally agreed with or did not comment on the recommendations. One agency agreed with one recommendation, but disagreed with another. The remaining agency disagreed with two recommendations. We subsequently removed one of these recommendations from the final report, but not the other. As of March 2018, all 39 recommendations remain open.

Implementing Key IT Workforce Planning Activities Can Help Ensure Acquisition Skill Gaps Are Addressed

An area where agencies can improve their ability to acquire IT is workforce planning. In November 2016, we reported[58] that IT workforce planning activities, when effectively implemented, can facilitate the success of major acquisitions. Ensuring program staff have the necessary knowledge and skills is a factor commonly identified as critical to the success of major investments. If agencies are to ensure that this critical success factor has been met, then IT skill gaps need to be adequately assessed and addressed through a workforce planning process.

In this regard, we reported that four workforce planning steps and eight key activities can assist agencies in assessing and addressing IT

[58] GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

knowledge and skill gaps. Specifically, these four steps are: (1) setting the strategic direction for IT workforce planning, (2) analyzing the workforce to identify skill gaps, (3) developing and implementing strategies to address IT skill gaps, and (4) monitoring and reporting progress in addressing skill gaps. Each of the four steps is supported by key activities (as summarized in table 3).

Table 3: Summary of Key Information Technology (IT) Workforce Planning Steps and Activities

Key workforce planning steps and activities
Set the strategic direction for IT workforce planning
Establish and maintain a workforce planning process
Develop competency and staffing requirements
Analyze the IT workforce to identify skill gaps
Assess competency and staffing needs regularly
Assess gaps in competencies and staffing
Develop strategies and implement activities to address IT skill gaps
Develop strategies and plans to address gaps in competencies and staffing
Implement activities that address gaps (including IT acquisition cadres, cross-functional training of acquisition and program personnel, career paths for program managers, plans to strengthen program management, and use of special hiring authorities)
Monitor and report progress in addressing IT skill gaps
Monitor the agency's progress in addressing competency and staffing gaps
Report to agency leadership on progress in addressing competency and staffing gaps

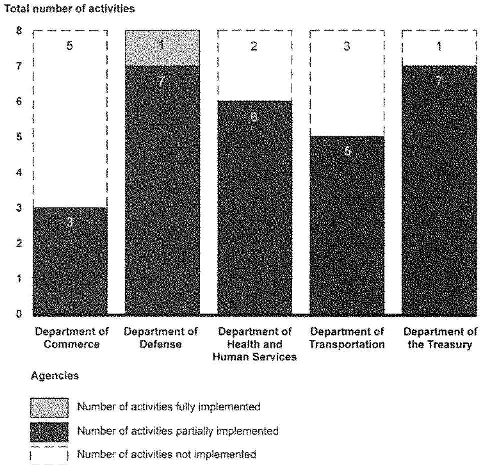
Source: GAO analysis of strategic human capital planning and IT workforce planning activities from sources including the Clinger-Cohen Act of 1996, E-Government Act of 2002, Federal Cybersecurity Workforce Assessment Act of 2015, and FITARA; OMB guidance including 25 Point Implementation Plan to Reform Federal Information Technology Management, Guidance for Specialized Information Technology Acquisition Cadres, Management and Oversight of Federal Information Technology (M-15-14), Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government (M-16-04), Federal Cybersecurity Workforce Strategy (M-16-15), and Circular A-130, Managing Information as a Strategic Resource; OPM guidance including IT Program Management Career Path Guide and Workforce Planning Model; and prior GAO reports, including GAO-04-39 and GAO-14-704G. | GAO-18-460T

However, in our November 2016 report, we determined that the five agencies that we selected for in-depth analysis had not fully implemented key workforce planning steps and activities.[59] For example, four of these agencies had not demonstrated an established IT workforce planning process. In addition, none of these agencies had fully assessed their workforce competencies and staffing needs regularly or established strategies and plans to address gaps in these areas. Figure 9 illustrates

[59] These five agencies are the Departments of Commerce, Defense, Health and Human Services, Transportation, and the Treasury.

the extent to which the five selected agencies had fully, partially, or not implemented key IT workforce planning activities.

Figure 9: Selected Agencies' Implementation of Eight Key Information Technology Workforce Planning Activities



Source: GAO analysis of agencies' data. | GAO-18-460T

The weaknesses identified were due, in part, to these agencies lacking comprehensive policies that required such activities, or failing to apply the policies to IT workforce planning. We concluded that, until these weaknesses are addressed, the five agencies risk not adequately assessing and addressing gaps in knowledge and skills that are critical to the success of major acquisitions. Accordingly, we made five recommendations to the five selected agencies to address the weaknesses in their IT workforce planning practices that we identified. Four agencies—the Departments of Commerce, Health and Human Services, Transportation, and the Treasury—agreed with our recommendations and one, the Department of Defense, partially agreed. As of March 2018, the agencies had not addressed the five recommendations.

Agencies Need to Address Aging Legacy Systems

IT investments across the federal government are becoming increasingly obsolete. Specifically, in May 2016, we reported that many agencies were using systems which had components that were, in some cases, at least 50 years old.[60] For example, we determined that the Department of Defense was using 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation's nuclear forces. In addition, the Department of the Treasury was using assembly language code—a computer language initially used in the 1950s and typically tied to the hardware for which it was developed. Further, in some cases, the vendors were no longer providing support for hardware or software. For example, each of the 12 agencies in our review reported using unsupported operating systems and components. At the time, five of the selected agencies reported using 1980s and 1990s Microsoft operating systems that stopped being supported by the vendor more than a decade ago. Table 4 provides examples of legacy systems across the federal government that agencies report are 30 years old or older and use obsolete software or hardware, and identifies those that do not have specific plans with time frames to modernize or replace these investments.

Table 4: Examples of Legacy Investments and Systems, as of May 2016

Agency	Investment or System	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of the Treasury	Individual Master File	The authoritative data source for individual taxpayers where accounts are updated, taxes are assessed, and refunds are generated. This investment is written in assembly language code—a low-level computer code that is difficult to write and maintain—and operates on an IBM mainframe.	~56	No - The agency has general plans to replace this investment, but there is no firm date associated with the transition.
Department of the Treasury	Business Master File	Retains all tax data pertaining to individual business income taxpayers and reflects a continuously updated and current record of each taxpayer's account. This investment is also written in assembly language code and operates on an IBM mainframe.	~56	No - The agency has general plans to update this system, but there is no time frame established for this transition.

[60] GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems,* GAO-16-468 (Washington, D.C.: May 25, 2016).

Agency	Investment or System	Description	Agency-reported age	Specific, defined plans for modernization or replacement
Department of Defense	Strategic Automated Command and Control System	Coordinates the operational functions of the United States' nuclear forces, such as intercontinental ballistic missiles, nuclear bombers, and tanker support aircraft. This system runs on an IBM Series/1 Computer—a 1970s computing system—and uses 8-inch floppy disks.	53	Yes - The agency plans to update its data storage solutions, port expansion processors, portable terminals, and desktop terminals by the end of fiscal year 2017.
Department of Veterans Affairs	Personnel and Accounting Integrated Data	Automates time and attendance for employees, timekeepers, payroll, and supervisors. It is written in Common Business Oriented Language (COBOL)—a programming language developed in the 1950s and 1960s—and runs on an IBM mainframe.	53	Yes - The agency plans to replace it with a project called Human Resources Information System Shared Service Center in 2017.
Department of Veterans Affairs	Benefits Delivery Network	Tracks claims filed by veterans for benefits, eligibility, and dates of death. This system is a suite of COBOL mainframe applications.	51	No - The agency has general plans to roll capabilities into another system, but there is no firm time frame associated with this transition.
Department of Justice	Sentry	Provides information regarding security and custody levels, inmate program and work assignments, and other pertinent information about the inmate population. The system uses COBOL and Java programming languages.	35	Yes - The agency planned to update the system through September 2016.
Social Security Administration	Title II Systems	Determines retirement benefits eligibility and amounts. The investment is comprised of 162 subsystems written in COBOL.	31	Yes - The agency has ongoing modernization efforts, including one that is experiencing cost and schedule challenges due to the complexities of the legacy software.

Source: GAO analysis of IT Dashboard data, agency documentation, and interviews. | GAO-18-460T

Note: Age was reported by agencies. Systems and investments may have individual components newer than the reported age.

To address this issue, we recommended that 12 agencies identify and plan to modernize or replace legacy systems, including establishing time frames, activities to be performed, and functions to be replaced or enhanced.[61] Most agencies agreed with our recommendations or had no comment. As of March 2018, all of the recommendations remained open.

In conclusion, the federal government has an opportunity to save billions of dollars; improve the transparency and management of IT acquisitions

[61] These 12 agencies are the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, the Treasury, Transportation, and Veterans Affairs, and the Social Security Administration.

and operations; and to strengthen the authority of CIOs to provide needed direction and oversight. The forum we held also recommended that CIOs be given more authority, and noted the important role played by the Federal CIO.

Most agencies have taken steps to improve the management of IT acquisitions and operations by implementing key initiatives, including data center consolidation, efforts to increase transparency via OMB's IT Dashboard, incremental development, management of software licenses, approval of IT acquisitions, implementation of IT workforce key practices, and addressing legacy IT; and they have continued to address recommendations we have made over the past several years. However, additional improvements are needed, and further efforts by OMB and federal agencies to implement our previous recommendations would better position them to improve the management of IT acquisitions and operations.

To help ensure that these efforts succeed, OMB's and agencies' continued implementation of recommendations is essential. In addition, we will continue to monitor agencies' implementation of our previous recommendations.

Chairmen Meadows and Hurd, Ranking Members Connolly and Kelly, and Members of the Subcommittees, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Dave Powner, Director, Information Technology at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Kevin Walsh (Assistant Director), Chris Businsky, Rebecca Eyler, Meredith Raymond, and Jessica Waselkow (Analyst in Charge).

Mr. HURD. Thanks for being an important partner on this.

And I misspoke. I apologize. Everybody has 5 minutes.

So, Ms. Weichert, you are now up for your 5 minutes.

STATEMENT OF THE HONORABLE MARGARET WEICHERT

Ms. WEICHERT. Thank you very much. It's great to be here on Pi Day to talk about this important subject.

So, Chairman Hurd, Ranking Member Kelly, and members of the subcommittees, thank you for the opportunity to appear before you today to discuss the state of Federal information technology in 2018.

In December, in testifying before the Senate Committee on Homeland Security and Governmental Affairs, I discussed the range of disciplines that the Deputy Director for Management is charged with overseeing, including IT, information security, human capital management, finance, accounting, performance management, and procurement.

Today, as the newly sworn-in Deputy Director for Management, I'm working with our agency partners to drive necessary improvement in those disciplines. And I'm excited to talk about one of those areas, IT modernization, in depth.

Improving our technology infrastructure is fundamental to aligning the executive branch to the mission, service, and stewardship needs of the 21st century. To that end, next week, we will release the President's Management Agenda, the PMA, an agenda which places IT modernization at its core.

The PMA sets out a long-term vision for more effective government that better achieves missions and enhances the key services upon which the American people depend. IT modernization must provide the essential backbone of the government service delivery while keeping sensitive data and systems secure. And the President's Management Agenda also links to related critical issues associated with data accountability and transparency as well as the people and workforce for the 21st century.

Since the establishment of the Office of E–Government and Information Technology in 2002, OMB has played a pivotal role in formulation of IT policy and strategic direction across the Federal Government. The Office of the Federal CIO, the Chief Information Security Office of the U.S., and the United States Digital Service are all in my organization. And, together, these groups leverage the convening authorities of OMB, including the CIO Council and the CISO Council, to coordinate executive-branch IT modernization activities.

In addition, since 2014, U.S. Digital Service has been focused on improving and transforming the experience of Americans who interact with government online. This means that more citizens can easily and seamlessly access government services online due to more secure identity-proofing. It means veterans are receiving appeals responses in a more timely manner. It has enhanced Medicare claims processing, allowing citizens to access health data online. And USDS has also helped made it easier for small businesses to compete for government contracts and for acquisition officers to be better positioned to acquire commercial technology. Ultimately, all this work is part of a broader strategy to help rebuild Americans' trust in government.

Today, I look forward to talking with you about a range of IT modernization initiatives, including the IT modernization report, the Modernizing Government Technology Act, Federal cybersecurity policy, agency IT transformation activities, including the work of U.S. Digital Service, and the IT workforce of the future, to name a few areas. More detailed background on many of these topics is included in my written testimony for the record.

And, in closing, OMB looks forward to working with the Oversight and Government Reform Committee and with Congress broadly on IT modernization. Over the years, this oversight committee has been instrumental in driving Federal IT modernization through its role in developing legislation such as FITARA, the DATA Act, and the MGT Act. Through our collaborative efforts, I know we will be able to improve government services and cybersecurity.

I thank the subcommittees for holding this hearing and for your commitment to IT modernization. I will be pleased to answer any questions you have.

[Prepared statement of Ms. Weichert follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/omb

TESTIMONY OF MARGARET WEICHERT
DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEES ON
INFORMATION TECHNOLOGY AND GOVERNMENT OPERATIONS OF THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

March 14, 2018

Chairman Hurd, Ranking Member Kelly, Chairman Meadows, Ranking Member Connolly, and Members of the Subcommittees, thank you for the opportunity to appear before you today to discuss the state of Federal information technology (IT) in 2018.

In December, I had the pleasure of testifying before the Senate Committee on Homeland Security and Governmental Affairs. At that time, I discussed the broad range of disciplines that the Deputy Director for Management is charged with overseeing, including IT, Information Security, Human Capital Management, Finance, Accounting, Performance Management and Procurement. Today, as the newly sworn in Deputy Director for Management, I am working with our agency partners to drive necessary improvement in those disciplines, and I am excited to talk about one of those core areas – IT modernization – in depth.

Improving our technology infrastructure to enhance the quality, security, and impact of services we deliver to taxpayers is fundamental to bringing the Executive Branch into the 21st Century. To that end, next week we will be releasing the President's Management Agenda (PMA), of which IT modernization is one of three pillars. The PMA will set forth a long-term vision for an effective Government that better achieves its missions and enhances the key services upon which the American people depend. Modernization is the essential backbone of how Government serves the public in ways that meet its needs, while keeping sensitive data and systems secure and private. IT modernization efforts directly support the other two pillars of the PMA – modernizing the government workforce to align staff skills with evolving mission needs, and delivering transparency through data to increase accountability.

The Office of Management and Budget (OMB) has always played a critical role in Government IT modernization, and this has been a core competency of OMB since the establishment of the Office of E-Government and Information Technology in 2002. The importance of IT in delivering results to the public has substantially increased since then. This Administration has therefore doubled down on the commitment to technology modernization. The United States Digital Service (USDS), also housed in OMB, has added capabilities to pursue IT modernization.

And, on May 1, 2017, the President established the American Technology Council (ATC) via Executive Order (E.O.) No. 13794, to effectuate the secure and efficient use of IT across the Government, and to serve as a primary convening body between Government and industry to ensure that the Executive Branch is leveraging commercial technology and best practices. Just days later, on May 11, 2017, the President signed Executive Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* to enhance cybersecurity risk management across the Government. OMB is the at the center of the work supporting both the American Technology Council and the implementation of Executive Order 13800, while driving performance and accountability for these initiatives across the Government.

Today I will talk about OMB's ongoing efforts to implement E.O. 13800, including the progress implementing the December 2017 *Report to the President on Federal IT Modernization*, as well as the work that OMB is doing to implement the Modernizing Government Technology Act and to oversee Federal cybersecurity.

IT Modernization Report

The American Technology Council published the Report to the President on Federal IT Modernization in December 2017. It recommends 50 crosscutting actions to improve the security posture of Federal agencies as they implement their IT modernization plans to address network consolidation/modernization and shared services. The Administration is making great progress toward implementing these actions, and the OMB team is collaborating with its interagency partners to reduce or remove barriers for agencies to leverage more modern, dynamic, commercially-available IT solutions. For example, OMB is actively working to identify efficient and effective service offerings for Cloud-based email and collaboration tools, which help facilitate the daily work of millions of Federal employees.

OMB is also developing policies to reduce agency reporting burdens and to securely deploy a modern IT infrastructure. We will be updating the policies governing the High Value Assets, Trusted Internet Connections, and Continuous Diagnostics and Mitigation programs, and revising the way we address identity management in the Federal Government. The goal is to better enable agencies to leverage dynamic, secure, and commercially available IT solutions by removing existing barriers. OMB will track the implementation of these policies through its management and budgetary oversight functions, and through the Modernize IT to

Increase Productivity and Security Cross-Agency Priority (CAP) goal that supports the forthcoming President's Management Agenda.

Implementation of the Modernizing Government Technology Act

The Oversight and Government Reform Committee has been instrumental in recent years in driving Federal IT modernization through its development of legislation such as FITARA and the DATA Act. Since it is Sunshine Week, a time where we celebrate open access to public information, I want to particularly recognize the influence the DATA Act has had in advancing Federal data transparency. We also greatly appreciate Chairman Hurd's introduction last year of the House version of the Modernizing Government Technology (MGT) Act, and the support that bill received from subcommittee members that contributed to its enactment as part of the FY 2018 National Defense Authorization Act. The MGT Act is designed to provide agencies flexible sources of funding required to meet high priority technology modernization goals. Successful implementation of this law is critical to the Administration's IT modernization agenda. In order to drive execution of the MGT Act, on February 27th OMB issued M-18-12, Implementation of the Modernizing Government Technology Act, describing actions agencies can take to utilize the Technology Modernization Fund (TMF) and the IT Working Capital Funds (WCFs) authorities. Together, the MGT provides additional flexibilities so

OMB and agencies have the financial resource mechanisms and technical expertise necessary to move the Government closer to leading industry practices in IT modernization. This will allow agencies to pivot their energy and attention away from traditional bureaucratic problems towards embracing technology opportunities, and will ultimately allow the Government to provide better, more secure, user-centered services to the American people.

When the TMF is funded, the interdisciplinary board of experts who oversee the fund will provide necessary resources to high-impact, mission-focused agency IT projects. OMB is working closely with agencies that wish to establish IT WCFs so they can utilize best practices generated as part of the TMF process to evaluate and fund agency IT modernization efforts that are agile, successful, and deliver meaningful change.

OMB itself must lead the way in ensuring that the money we spend on our own personnel and service -- whether it is USDS, the Office of E-Government, or our other cross cutting management offices -- delivers the type of results expected by our agency partners, Congress and the American people. We are also looking to make more strategic use of the IT Oversight and Reform (ITOR) fund to direct expenditures and personnel to our highest technology priorities and make sure that lessons learned from interacting with agencies and helping them solve their problems informs our longer term policy development and modernization efforts.

USDS Support of Technology Modernization Efforts

Since 2014, USDS has been an OMB component that effectively enhances Government service delivery to the American people through technology and design. USDS is focused on improving and transforming the experience of Americans who interact with the Government online. This means more citizens are able to access more Government services online due to more streamlined and secure methods of identity verification. It means veterans receiving appeals responses in a more timely manner. This work can ultimately help rebuild Americans' trust in Government. In addition to its work with individual federal agencies, USDS delivers projects such as the TechFAR Hub, a website that brings industry best practices to federal digital service acquisition, helping the Federal government to build the knowledge it needs to modernize its procurement strategy.

Cybersecurity

Far-reaching cybersecurity incidents of 2017 demonstrate the potentially harmful impact that insufficient cybersecurity can have on our Nation. Hundreds of millions of Americans had their personally identifiable information (PII) compromised in a series of private sector data breaches that exploited unpatched vulnerabilities at companies whose core services focus on safeguarding that very information. Tens of thousands of Federal employees and taxpayers also had their information compromised because of vulnerabilities in agencies' data and system protections. These incidents continue to demonstrate that effective cybersecurity requires any organization — whether it be a Federal agency or other public or private company — to identify, prioritize, and manage cyber-risks across its enterprise.

The President signed Executive Order 13800 in May 2017 to enhance cybersecurity risk management across the Federal Government. E.O. 13800 recognizes that the Government must ensure that it is able to properly secure citizens' information and that agencies can protect their systems even as malicious cyber actors seek to disrupt their services. Accordingly, E.O. 13800 requires every agency to conduct comprehensive reviews of their cybersecurity programs. The order also directs OMB, Department of Homeland Security (DHS), Department of Defense, Department of Commerce, and several other key agencies to review cybersecurity practices across the Government and critical infrastructure sectors. E.O. 13800 assesses the sufficiency of agencies' risk mitigation and acceptance choices and includes a plan for remediating cybersecurity performance gaps. In implementing E.O. 13800, OMB determined that agencies lack sufficient situational awareness of the threat environment, capabilities to adequately detect intrusions and data exfiltration, and fundamental accountability for mitigating cyber risks across the enterprise.

While E.O. 13800 is part of the roadmap for securely modernizing Federal IT systems over the coming years, our Modernize IT Cross Agency Priority (CAP) goal will establish meaningful metrics that focus on cybersecurity capabilities that reduce cyber risks to agency missions, the most tangible return on investment that we can demonstrate. The CAP goal emphasizes long-standing efforts of OMB and DHS to enforce disciplined, risk-based, cyber practices across Government, and to help safeguard agency IT systems, including helping agencies to address critical vulnerabilities and implement multi-factor authentication. Progress to date is encouraging, but insufficient. Agencies endured 35,277 cybersecurity incidents in Fiscal Year (FY) 2017, a 14% increase over the 30,899 incidents that agencies reported in FY 2016. Modernizing our IT Infrastructure will reduce the risk of crucial services being disrupted. Toward this end, the $15 billion cybersecurity budget request submitted as part of the President's FY 19 Budget would fund investment in critical capabilities to safeguard agency IT assets and data. OMB's data-driven oversight of agency programs directly informed this request level.

Also essential are the current and future Federal workers needed to help implement these critical capabilities. The nation's growing challenges require a capable Federal technology and cybersecurity workforce that possesses the necessary knowledge, skills, and competencies to counter increasingly sophisticated and ever-changing threats. I am working with the Office of Personnel Management, DHS, the National Institute of Standards and Technology (NIST), and agencies across the Executive Branch on government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats.

Closing

In closing, OMB looks forward to working with Congress on IT modernization. Through our collaborative efforts, we will be able to improve Government services and cybersecurity. I thank the Subcommittees for holding this hearing, and for your commitment to IT modernization. I would be pleased to answer any questions you may have.

Mr. HURD. Thank you.

Mr. Zielinski, you are now recognized for 5 minutes.

STATEMENT OF BILL ZIELINSKI

Mr. ZIELINSKI. Great. Good afternoon, Chairman Hurd, Ranking Member Kelly, and members of the subcommittee. My name is Bill Zielinski, and I am the Deputy Assistant Commissioner for the Office of Information Technology Category in GSA's Federal Acquisition Service. In addition, I also serve as the Office of Management and Budget-appointed government-wide IT category manager.

I am pleased to be here today to discuss the important role GSA plays in Federal information technology efforts government-wide.

The IT Category at GSA enables agencies in the acquisition of $50 billion in goods and services annually from more than 20,000 industry partners. ITC's top priority is to maximize customer value and mission productivity.

And while GSA brings significant capabilities to the table in facilitating the modernization of the Federal Government's IT infrastructure and applications, it's through the strategic partnerships with other agencies and our industry partners where we will make the greatest progress.

For instance, I work closely with OMB's Office of Federal Procurement Policy and administrator of the Office of Electronic Government to review the Federal IT spend, determine where opportunities exist to collaborate on the acquisition of IT products and services, and implement strategies to get more value from IT dollars.

In that vein, I would now like to discuss four key ways in which GSA is supporting the modernization of the Federal Government's IT infrastructure and applications.

First, in December, the American Technology Council issued its final report to the President on Federal IT modernization. The report is the culmination of a months-long process to develop a strategic plan that approves the security posture of Federal IT and incorporates feedback from industry and members of the public.

The report has three key objectives that will inform future efforts: to reduce the Federal attack surface through enhanced application and data-level protections; to improve visibility beyond the network level; and to ensure that policy, resource allocation, acquisition, and operational approaches to security enable the use of new technology without sacrificing reliability or performance.

GSA is directly tasked, in whole or in part, with half of the 50 action items recommended by the report and is actively working on these deliverables in accordance with report timelines.

Second, the MGT Act is another critical tool for modernizing Federal IT. GSA thanks the members of these subcommittees for their dedication to getting this legislation passed.

GSA is tasked with several key actions related to the MGT's Technology Modernization Fund. Chief among them is providing broad support for the Technology Modernization Board's activities, including technical support and the monitoring of agencies that receive funds from the TMF. Subject to appropriations, the GSA is prepared to help administer this critically important fund.

Third, in partnership with the White House Office of American Innovation, GSA is working to establish five new centers of excellence. The COEs will house centralized function-specific talent, products, and acquisition vehicles. These teams will provide expert advice, development resources, and support solution implementation in the areas of cloud adoption, IT infrastructure optimization, customer experience, service delivery analytics, and contact centers. The first client agency for the COEs is the United States Department of Agriculture.

Finally, GSA is helping agencies adopt new approaches for buying commercial off-the-shelf and as-a-service solutions. By leading in the development of modular contracting approaches to enable agile and efficient development of complex, new requirements, we are able to assist agencies through the entire lifecycle of procurement and system development.

GSA's unique mix of talent and expertise in acquisition technology and service delivery, combined with our government-wide scope and scale, makes our agency an agent of transformation in how agencies will buy, build, and use technology.

I want to thank you for the opportunity to appear before you today to discuss GSA's role, and I look forward to answering your questions.

[Prepared statement of Mr. Zielinksi follows:]

Statement of William Zielinski
Deputy Assistant Commissioner of the IT Category, U.S. General Services Administration
Before the Subcommittees on Information Technology
and Government Operations of the
Committee on Oversight and Government Reform
March 14, 2018 at 2:00 p.m.
2154 Rayburn House Office Building

State of Play: Federal IT in 2018

Chairmen Hurd and Meadows, Ranking Members Kelly and Connolly, and members of the subcommittees, my name is Bill Zielinski, and I am the Deputy Assistant Commissioner for the Office of Information Technology Category (ITC) in the General Services Administration's (GSA) Federal Acquisition Service (FAS). In addition, I also serve as the Office of Management and Budget (OMB) appointed, governmentwide Information Technology (IT) Category Manager. I am pleased to be here today to discuss the important role GSA plays in federal information technology efforts governmentwide.

The modernization of the federal government's IT infrastructure and applications is an important priority for GSA. We are supporting governmentwide modernization in four ways that I will introduce here and discuss further in my testimony.

1. First, in partnership with the President's Office of American Innovation, GSA's Technology Transformation Services (TTS) team is standing up IT Modernization Centers of Excellence.
2. Second, we are leading a number of key initiatives identified in the recently issued Report to the President on Federal IT Modernization.
3. Third, we are well positioned to support the operation and administration of the recently established Technology Modernization Fund.
4. Fourth and finally, GSA is modernizing and simplifying the systems we use to serve our agency customers in the acquisition of $50 billion in goods and services annually from more than 20,000 industry partners.

For those unfamiliar with GSA's Office of Information Technology Category, we deliver flexible IT solutions and services that support agency missions, and drive innovative and agile improvements through Category Management. ITC's top priority is to maximize customer value and mission productivity by:

> Providing all agencies a suite of solutions at any maturity level using our technological and acquisition expertise — our office facilitates $23 billion in annual government spend and 98 percent of federal agencies utilized our contract vehicles last year.
>
> Working with agencies and suppliers to make emerging, transformative technology, and innovations available governmentwide, while fostering small business participation. Small businesses have won nearly $8 billion of spend (38 percent of total dollars won) through ITC.
>
> And, reducing the number of duplicative contracts through focused vendor management efforts — such as GSA's successful effort to consolidate the Professional Services

Schedule, reducing the number of individual services contracts our industry partners have to maintain.

Under the IT Category, ITC is focused on five IT Subcategories:

1. The **IT Hardware** Subcategory works to stay on the forefront of technology information, innovative products, and emerging trends, and is comprised of purchase, lease, and maintenance options for communications and computing equipment, other electronics and fiber optics, as well as hardware services.

2. The **IT Security** Subcategory serves as a resource to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

3. The **IT Services** Subcategory is comprised of IT Outsourcing and IT Consulting and plays a significant role in achieving the federal government's category management goals: to improve the acquisition and management of common IT goods and services to drive mission delivery, greater performance and efficiencies, and cost savings.

4. The **IT Software** Subcategory is comprised of Infrastructure Software, Enterprise Application Software, as well as Licensing and Maintenance.

5. The **Telecommunications** Subcategory includes networks, mobile and wireless, and satellites. Government services built upon the government telecom infrastructure include humanitarian relief, disaster-response, counter-terrorism efforts, healthcare IT, and more.

As a brief, real world example of our work: last year, one of our customers needed computers for Hurricanes Harvey and Irma relief efforts - and they needed them quickly. We facilitated the procurement of 1,000 laptops to assist with the recovery efforts. The order resulted in a reduced delivery time and $75,000 in savings when compared to the awarded Blanket Purchase Agreement (BPA) price, and was awarded to a women-owned, 8(a) small business under IT Schedule 70 (a Best-In-Class vehicle).

Governmentwide Coordination Efforts

While GSA brings significant capabilities to the table in facilitating the modernization of the federal government's IT infrastructure and applications, it is through the strategic partnerships with other agencies where we will be able to make the greatest progress. I will highlight a few of those partnerships:

I work in close coordination with OMB's Office of Federal Procurement Policy (OFPP) and the Office of Electronic Government (eGov) to review Federal IT spend, determine where opportunities exist to collaborate on the acquisition of IT products and services and implement IT Category strategies to improve outcomes and get more value from IT dollars.

For example, in developing the Enterprise Infrastructure Solutions (EIS) contract to provide vital network capabilities for agencies to accomplish their missions, we partnered closely with the Department of Homeland Security (DHS) to ensure that solutions provided by vendors will meet the rigorous security requirements needed to protect vital IT assets.

The Mobile Services Category Team (MSCT) involves a healthy and thriving governmentwide community, led by OMB, GSA, DHS, the Department of State, and the Department of Defense (DOD). MSCT provides guidance, strategies, and practical solutions to grow and evolve mobility capabilities to meet the growing demands in this marketplace.

Additionally, GSA partnered closely with DHS and the National Institute of Standards and Technology (NIST) at the Department of Commerce in the development of the Highly Adaptive Cybersecurity Services (HACS) acquisition solution. This procurement vehicle provides agencies with access to qualified providers of IT security capabilities to improve agency security posture on High Value Assets (HVAs).

These are just a few examples and, moving forward, we are aligning our efforts to the Administration's IT Modernization Report and the intent of the Modernizing Government Technology (MGT) Act to provide a more modern and secure Federal IT enterprise.

Key Recent Developments

Several recent examples of the Administration's commitment to upgrading federal IT are worth expounding upon:

First, on December 13, 2017, the American Technology Council (ATC) issued a final "Report to the President on Federal IT Modernization" from the Secretary of Homeland Security, the Director of OMB, and the Administrator of GSA in response to Executive Order 13800. The report is the culmination of a months-long process coordinated by the ATC to develop a strategic plan that improves the security posture of Federal IT, and incorporates feedback from dozens of comments received from industry and members of the public. The report recognizes that Federal IT practices must undergo fundamental, non-incremental change to successfully modernize something as large and complex as Federal government IT. The report contains three key objectives that will inform future federal efforts on Federal IT modernization:

- Reduce the Federal attack surface through enhanced application and data-level protections;
- Improve visibility beyond the network level; and
- Ensure that policy, resource allocation, acquisition, and operational approaches to security enable use of new technology without sacrificing reliability or performance.

In order to achieve these efforts, 50 action items are delineated; GSA is directly tasked, in whole or in part, with 25 of the 50 action items recommended by the report. GSA is actively working on these deliverables in accordance with the timelines in the report.

Another critical tool for modernizing Federal IT was provided by Congress recently when it passed the MGT Act as part of the National Defense Authorization Act for Fiscal Year 2018 (P.L. 115-91), which the President signed into law on December 12, 2017. GSA thanks the members of these subcommittees for their dedication to getting this legislation across the finish line.

The MGT Act contains two major provisions - the first allows agencies to establish working capital funds for the purposes of undertaking critical IT modernization projects such as transitioning from legacy systems to the cloud or improving an agency's cybersecurity posture;

and the second creates a Technology Modernization Fund (TMF), administered by GSA in accordance with OMB guidance and with input from a Technology Modernization Board, to fund "technology-related activities, to improve information technology, [and] to enhance cybersecurity across the Federal Government."

GSA is tasked with several key actions related to the TMF, chief among them is providing broad support for the Board's activities, including technical support and monitoring agencies that receive funds from the TMF. Subject to FY 18 appropriations, GSA is prepared to help administer this critically important fund.

Third, GSA's Federal Acquisition Service (FAS), in partnership with the White House Office of American Innovation, is working to establish five new Centers of Excellence (COE). The COEs will house centralized, function specific talent, products and acquisition vehicles. Agencies have unique missions but the systems they build to deliver those missions rely on foundational capabilities that are not unique. The COE teams will provide expert advice, consulting, development and support solution implementation in the following areas:

- **Cloud Adoption -** Perform application/system portfolio analysis, develop cloud migration recommendations, plan and manage the migration execution, as well as capture specific capabilities (e.g. strategies, roadmaps, playbooks) to document good practices across government. The goal is to assist agencies accelerate cloud adoption.
- **IT Infrastructure Optimization -** Assist agencies with the assessment, development and implementation of computing infrastructure (i.e. network, storage, data center) optimization plans.
- **Customer Experience -** Assist agencies with the development and implementation of an optimal client experience strategy. Implementation will include utilization of the latest technology (artificial intelligence, learning systems, and robotic process automation) as well as a cohesive client experience across all channels including contact centers, online platforms, informational materials, and in-person interactions.
- **Service Delivery Analytics -** Provide the expertise and tools to define, instrument and analyze ultimate program outcomes, customer experiences and operational effectiveness. Aim to ensure programs and services are designed and delivered in a way that optimizes impact while building trust and confidence in the public. Implementation includes a continuous improvement feedback cycle built into services delivered.
- **Contact Center -** Provide a suite of offerings to help agencies manage and enhance their customer contacts where they need assistance the most, be it with managing their contact center operations; building self-service tools; leveraging robotic process automation and emerging technologies; building internal business processes and systems to manage day-to-day performance; navigating available acquisition solutions; and learning contact center best practices.

The first client agency for the COEs is the United States Department of Agriculture (USDA). After a successful Industry Day at the White House in December, GSA has been assembling the teams that will comprise the five COEs.

Expectations for 2018

Technology is critical to how every agency accomplishes its mission and serves the public. It is at the core of running mission-support operations, safeguarding critical information, and analyzing program data for agency decision making.

The challenge of supporting, managing, and securing legacy systems significantly affects the ability of Federal agencies to meet current and evolving mission requirements. GSA is leading a modernization that rethinks business problems and uses new, innovative technologies and IT practices to help Government IT work better. GSA and its agency partners have the capabilities to shift more Federal IT spending from maintenance to modernization.

GSA is helping agencies adopt new approaches for buying commercial-off-the shelf and as-a-service solutions. We are leading the development of modular contracting approaches to enable agile and efficient development of complex new requirements. GSA's goal is to assist agencies through the entire life cycle of procurement and system development.

Keeping up with the public's expectations for services, and digital services in particular, is one of GSA's key focuses. The latest American Customer Satisfaction Index (ACSI), shows the Federal Government making progress. After several years of declining satisfaction, 2016 saw a six-point jump. ACSI stated that "while several factors combine to explain the rise in satisfaction over the last 12 months, the improvement for Government websites stands out." GSA is a leader in improving Government websites and making customer experiences simple, fast, and secure.

The technology challenges facing Federal agencies and the direct impact on the public are well-known by leaders across Government and the private sector. In partnership with the Office of American Innovation and the American Technology Council in the White House, GSA will be an essential partner in providing solutions through the Centers of Excellence, the IT Category, and the Office of Governmentwide Policy. Our unique mix of talent and expertise in acquisition, technology, and service delivery - combined with our governmentwide scope and scale - make GSA an agent of transformation in how Federal agencies buy, build, and use technology.

Thank you for the opportunity to appear before you today to discuss GSA's role in federal IT modernization efforts. I look forward to answering any questions you have.

Mr. HURD. Thank you.

And, Ms. Manfra, you are now recognized for 5 minutes for your opening remarks.

STATEMENT OF THE HONORABLE JEANETTE MANFRA

Ms. MANFRA. Thank you.

Chairman Hurd, Ranking Member Kelly, members of the committee, thank you for today's opportunity to discuss the Department of Homeland Security's efforts to secure Federal networks.

I would like to begin my testimony by thanking Congress for its work on the Cybersecurity and Infrastructure Security Agency Act of 2017. If enacted, this legislation will streamline the National Protection and Programs Directorate, or NPPD, and rename our organization to more clearly reflect our central role in government and private-sector critical infrastructure security. Much progress has been made, but we must stay focused until this work is complete. The Department strongly supports this effort and encourages swift action by Congress.

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Over the past year, Federal network defenders saw the threat landscape grow more crowded, active, and dangerous. While in many cases our defenses have been successful in mitigating these threats, we must do more to ensure our cyber defenses keep pace of technological change and evolving risk.

In my role at DHS, I head the Office of Cybersecurity and Communications. A core part of my role is protecting and managing the overall information security of Federal civilian networks. To do this, we must first gain visibility to understand the exposure that the Federal enterprise faces. Then we need to use our authorities to reduce this risk, whether that's through directives, guidance, or direct support to agencies. And, finally, we must build capacity within agencies to implement our guidance, act on threat information, and fully leverage the capabilities and services that DHS has to offer.

Programs like the National Cybersecurity Protection System, or EINSTEIN, and the Continuous Diagnostics and Mitigation Program directly serve and enable these three lines of effort.

Last year, the President signed an executive order on strengthening the cybersecurity of Federal networks and critical infrastructure, which set in motion a series of assessments and deliverables to improve our defenses and lower our risk to cyber threats.

Across the Federal Government, agencies have been implementing the NIST Cybersecurity Framework. Agencies have been reporting to DHS and OMB on their cybersecurity risk mitigation and acceptance choices. DHS and OMB have evaluated the totality of these agencies' reports in order to comprehensively assess the Federal Government's cybersecurity risk management posture.

The assessment found the Federal enterprise to be at risk. The choices we make to reduce this risk, in both cybersecurity budget and operational priorities, must be informed by a data-driven, risk-based assessment of Federal cybersecurity and the threat environment.

As part of the executive order, my office has been working with OMB, GSA, and Federal agencies to modernize the Federal Government's IT infrastructure. We are exploring opportunities to consolidate network architectures, embrace shared IT services, all the while emphasizing cybersecurity as a foundational element to all new IT services.

We recognize that legacy IT systems present considerable challenges in efforts to secure Federal networks. The risks posed by these antiquated, end-of-life systems has perhaps best been demonstrated by the difficulties agencies face in complying with DHS's binding operational directives which govern vulnerability patching. Some legacy systems can no longer be patched, others are not supported by vendors, and some experience significant performance issues if not reconfigured during the security upgrade process.

While in most cases DHS and the agencies have been able to address these issues and either upgrade, transition, or mitigate the problem entirely, this complicates and adds cost to agency efforts to patch their own systems—an exercise that does need to be as painless as possible.

While the use of more modern IT has efficiencies and convenience of its own, the benefits it brings to cybersecurity efforts are also significant.

My organization works with departments and agencies to identify and prioritize high-value assets or those systems for which a cyber incident could cause significant impact to the United States. We conduct security architecture reviews to assess network architectures and configurations and conduct in-depth vulnerability assets, which determine how an adversary could compromise these systems, persist in their networks, and gain access to sensitive data.

These assessments provide system owners with recommendations to address identified vulnerabilities and assist them in prioritizing their limited resources to fix the worst things first.

In closing, I want to assure this committee that DHS is embracing our statutory responsibility to administer the implementation of Federal agency cybersecurity policies and practices by leading the effort to secure the Federal enterprise, in coordination with my partners on the panel, following a risk-based approach.

This committee played a key role in championing the passage of FISMA 2014 and clarifying these important authorities for DHS, and we thank you for those.

The overarching goal of Federal cybersecurity is to ensure that every agency maintains an adequate level of cybersecurity commensurate with its own risk and with those of the Federal enterprise.

Thank you for the opportunity to testify, and I look forward to any questions you may have.

[Prepared statement of Ms. Manfra follows:]

Statement for the Record

of

Jeanette Manfra
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
U.S. House of Representatives
Subcommittee on Information Technology
Subcommittee on Government Operations
Committee on Oversight and Government Reform

Regarding

State of Play: Federal IT in 2018

March 14, 2018

Chairman Hurd, Chairman Meadows, Ranking Member Kelly, Ranking Member Connolly, and members of the Subcommittees, thank you for today's opportunity to discuss the state of federal cybersecurity. The Department of Homeland Security (DHS) serves a critical role in safeguarding and securing cyberspace, a core homeland security mission. The National Protection and Programs Directorate (NPPD) at DHS leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. This past December, the House voted favorably on H.R. 3359, the "Cybersecurity and Infrastructure Security Agency Act of 2017." If enacted, this bill would mature and streamline NPPD, renaming our organization as the Cybersecurity and Infrastructure Security Agency to clearly reflect our essential mission and role in securing cyberspace. The Department strongly supports this much-needed legislation and encourages swift action by Congress to complete its work on this legislation.

NPPD is responsible for collaborating with federal agencies to protect civilian federal government networks, as well as with the Intelligence Community; law enforcement; state, local, tribal, and territorial governments; and the private sector to defend against cyber threats. We endeavor to enhance cyber threat information sharing across the globe to stop cyber incidents before they start and help businesses and government agencies to protect their cyber systems and quickly recover should such an incident occur. By bringing together all levels of government, the private sector, international partners, and the public, we are taking action to protect against cybersecurity risks, improve our whole-of-government incident response capabilities, enhance information sharing on best practices and cyber threats, and strengthen resilience.

Threats

Cyber threats remain one of the most significant and constant strategic risks for the United States, putting our national security, economic prosperity, and public health and safety at risk. We have long been confronted with a myriad of attacks against our digital networks. But over the past year, Americans saw malicious actors, including hackers, cyber criminals, and nation states, increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy.

Global cyber incidents, such as the "WannaCry" ransomware incident and the "NotPetya" malware incident in May and June 2017, respectively, are examples of malicious actors leveraging cyberspace to create disruptive effects and cause economic loss. These incidents exploited known vulnerabilities in software commonly used across the globe. Prior to these events, NPPD had already taken actions to help protect networks. Through vulnerability scanning, NPPD helped federal agencies and other stakeholders identify vulnerabilities on their networks so they could be patched before the incidents occurred. Recognizing that not all users are able to install patches immediately, NPPD shared additional mitigation guidance to assist network defenders.

Since 2009, cyber actors of the North Korean government have targeted the media, aerospace, financial, and critical infrastructure sectors in the United States and globally. The

U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. DHS and FBI have generated analytic products to provide information to network defenders to assist with the detection of malicious network activity. The analytic products provide technical details on the tools and infrastructure used by cyber actors of the North Korean government. Working with U.S. Government partners, DHS and FBI identified Internet Protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea's distributed denial-of-service (DDoS) botnet infrastructure. These actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote access tools (RATs), and wiper malware. Variants of malware and tools used by HIDDEN COBRA actors include Destover, Wild Positron/Duuzer, and Hangman. DHS previously released a technical alert, which contains additional details on the use of a server message block (SMB) worm tool employed by these actors. Further research is needed to understand the full breadth of this group's cyber capabilities. DHS and FBI assess that HIDDEN COBRA actors will continue to use cyber operations to advance their government's military and strategic objectives.

In another series of incidents since at least May of last year, working with U.S. and international partners, DHS and FBI have identified advanced persistent threat actors targeting government entities and businesses in the energy, nuclear, water, aviation, and critical manufacturing sectors. DHS assesses that this campaign comprises two distinct categories of victims: staging and intended targets. In other words, through DHS's incident response actions, we have observed this advanced persistent threat actor target certain entities that then become pivot points, leveraging existing relationships between the initial victim and the intended targets to hide their activity, as part of a multi-stage intrusion campaign to gain access to networks of major, high-value assets that operate components of our Nation's critical infrastructure. Based on DHS analysis and observed indicators of compromise, DHS has confidence that this campaign is still ongoing, and threat actors are actively pursuing their ultimate long-term campaign objectives. In recent weeks, DHS and the FBI remain active with incident response and have published a joint technical alert to enable network defenders to identify and take action to reduce exposure to this malicious activity.

Cybersecurity Priorities

This Administration has prioritized protecting and defending our public and economic safety from the range of threats that exist today, including those emanating from cyberspace. Last year, the President signed Executive Order (EO) 13800, on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Executive Order set in motion a series of assessments and deliverables to understand how to improve our defenses and lower our risk to cyber threats. This order also emphasized the importance of accountability – clarifying that agency heads are responsible and will be held accountable for the security of their networks and systems. NPPD plays an important role in providing capabilities, services and direction to federal agencies.

As part of the EO, NPPD has been working with our interagency partners to modernize the federal government's information technology (IT) infrastructure. This Committee has led this effort by working to enact the Modernizing Government Technology Act last December. We are exploring opportunities to consolidate network architectures and embrace shared IT services, while emphasizing cybersecurity is a foundational element of all new IT services. As federal agencies begin to leverage cloud computing and mobile technologies, we acknowledge that security solutions need to evolve. DHS is focused on the objectives that Trusted Internet Connections (TIC) mandate expected to achieve, such as gaining situational awareness across the federal civilian landscape, as opposed to driving a specific technical approach. We will continue our work with the Office of American Innovations, Office of Management and Budget and the federal civilian agencies to ensure agencies understand their roles and responsibilities to secure their data, maintain situational awareness and have appropriate security protections for their cloud environments. We must work quickly to replace legacy IT. No amount of investment in innovative cybersecurity capabilities will fully succeed in protecting our IT until we address the pervasive problem of legacy equipment and software across the federal enterprise. We must also modernize how the government manages IT risk in order to ensure effective, sustainable and secure investments. As such, we are taking steps to ensure that our investment planning and prioritization in future capabilities are driven by a threat informed approach. Leveraging the legislation passed by this committee, we are working with the agencies to modernize their systems.

The challenges posed by antiquated, end-of-life, legacy Federal IT systems has been apparent in the implementation of DHS's binding operational directives (BODs). Some legacy systems can no longer be patched, others are not supported by vendors, and some experience significant performance issues if not re-configured during the security upgrade/enhancement process. Many of these legacy systems simply were not designed for the current environment and the need for modern security approaches. As an example, during the implementation of BOD 15-01 (Mitigating Critical Vulnerabilities) and BOD 16-02 (Securing Network Infrastructure Devices), the DHS team identified and monitored dozens of end-of-life systems preventing the agency from quickly securing the system based on the BOD action. Fortunately, in most cases, DHS and the agency were able to address these issues and either upgrade, transition, or mitigate. While the use of more modernized IT equipment has many benefits for users and administrators, the benefits to cybersecurity are significant.

Across the Federal government, agencies have been implementing action plans to use the industry-standard Department of Commerce's National Institute of Standards and Technology Cybersecurity Framework. Agencies are reporting to DHS and the Office of Management and Budget (OMB) on their cybersecurity risk mitigation and acceptance choices. In coordination with OMB, NPPD has been evaluating the totality of these Agency reports in order to comprehensively assess the adequacy of the Federal government's overall cybersecurity risk management posture. DHS works with agencies and OMB to ensure agencies have adequate resources to address their cybersecurity risk.

DHS is embracing our statutory responsibility to administer, in consultation with OMB, the implementation of federal agency cybersecurity policies and practices by leading the effort to secure the federal civilian executive branch enterprise following a risk-based approach. This committee played a key role in championing the passage of FISMA 2014 and clarifying these important authorities for DHS. The overarching goal of federal cybersecurity is to ensure that every agency maintains an adequate level of cybersecurity, commensurate with its own risks and with those of the federal enterprise. E.O. 13800 makes clear that cybersecurity risk within the Executive Branch shall be managed as an enterprise. At the same time, agencies implement their cybersecurity programs and manage their own risk, as they are best positioned to understand how their unique mission environments need to be protected.

DHS supports these efforts by providing shared services and essential architecture and, along with the OMB, ensuring an adequate level of security enterprise-wide, including addressing systemic risks and interdependencies. We are working to assess risks at agencies, particularly systemic risks that could affect the Executive Branch as a whole; making recommendations to agencies and adjusting government-wide policies as necessary; making budgeting recommendation to OMB to ensure that cybersecurity risks are appropriately accounted for and funded; and furthering our analysis support to OMB to ensure that policies are adhered to and agencies are held accountable.

Our efforts, in collaboration with the Office of Management and Budget (OMB) and the General Services Administration, are guided by three principles: risk-based, cost-effective, and scalable. DHS addresses the greatest risks first and focuses on the highest impact systems, assets, and capabilities through cost-effective and scalable approaches. DHS leads through direct action and offerings, but also through collaboration and communication with agencies and partners, such as OMB, the General Services Administration, and the National Institute of Standards and Technology.

Cybersecurity Protections for Federal Networks

Although federal agencies have primary responsibility for their own cybersecurity, DHS, pursuant to its various authorities, provides a common set of security tools across the civilian executive branch and helps agencies manage their cyber risk. NPPD's assistance to federal agencies includes:

- providing tools to safeguard civilian executive branch networks through the National Cybersecurity Protection System (NCPS), which includes "EINSTEIN", and the Continuous Diagnostics and Mitigation (CDM) programs;
- measuring and motivating agencies to implement policies, directives, standards, and guidelines;
- serving as a hub for information sharing and incident reporting; and
- providing operational and technical assistance, including threat information dissemination and risk and vulnerability assessments, as well as incident response services.

NPPD's National Cybersecurity and Communications Integration Center (NCCIC) is the civilian government's hub for cybersecurity information sharing, asset incident response, and coordination for both private sector and the federal government.

EINSTEIN is a signature-based intrusion detection and prevention capability that takes action on known malicious activity, protecting unclassified networks at the perimeter of each federal government agency. EINSTEIN provides situational awareness of civilian executive branch network traffic, so threats detected at one agency are shared with all others providing agencies with information and capabilities to more effectively manage their cyber risk. We could not achieve such situational awareness through individual agency efforts alone.

NPPD is also leveraging investments in EINSTEIN to move beyond current reliance on signatures through pilot projects that are yielding positive results in the discovery of previously unidentified malicious activity. The pilot efforts are helping us to define the future operational needs for tactics, techniques, procedures, and skill sets required to operationalize the non-signature based approach to cybersecurity.

EINSTEIN will not block every threat; therefore, it must be complemented with systems and tools working inside agency networks—as effective cybersecurity risk management requires a defense-in-depth strategy that cannot be achieved through only one type of tool. CDM provides cybersecurity tools and integration services to all participating agencies to enable them to improve their respective security postures by reducing the attack surface of their networks as well as providing DHS with enterprise-wide visibility through a common federal dashboard.

CDM is helping us achieve two major advances for federal cybersecurity.

First, agencies are gaining visibility, often for the first time, into the extent of cybersecurity risks across their entire network. With enhanced visibility, they can prioritize the mitigation of identified issues based upon their relative importance.

Second, with the federal dashboard, the NCCIC will be able to operationalize this visibility, initially through improved vulnerability management. For example, the NCCIC currently tracks government-wide progress in implementing critical patches via agency self-reporting and manual data calls. CDM will transform this, enabling the NCCIC to immediately view the prevalence of a given software product or vulnerability across the federal government so that the NCCIC can provide agencies with timely guidance on their risk exposure and recommended mitigation steps.

Effective cybersecurity requires a robust measurement regime, and robust measurement requires valid and timely data. CDM will provide this baseline of cybersecurity risk data to drive improvement across the civilian executive branch.

DHS conducts a number of activities to measure agencies' cybersecurity practices and works with agencies to improve risk management practices. The Federal Information Security Modernization Act of 2014 (FISMA) provided the Secretary of Homeland Security with the authority to develop and oversee implementation of BOD to agencies. In 2016, the Secretary issued a BOD on securing High Value Assets (HVA), or those assets, federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. NPPD works with interagency partners to identify and prioritize HVAs for assessment and remediation activities across the federal government. For instance, NPPD conducts security architecture reviews on these HVAs to help agencies assess their system architecture and configurations. DHS has also coordinated with NIST to develop and issue an HVA Control Overlay. This guidance articulates specific guidance for implementing security controls that HVA system owners should implement, in addition to existing controls they have selected, to mitigate against known threats and weaknesses.

In addition to security architecture reviews, DHS conducts in-depth vulnerability assessments of the priority agency HVAs to determine how an adversary could penetrate a system, move around an agency's network to access sensitive data, and exfiltrate such data without being detected. These assessments include services such as penetration testing, wireless security analysis, and "phishing" evaluations in which NPPD cyber operators send emails to agency personnel and test whether recipients click on potentially malicious links. NPPD has focused these assessments on federal systems that may be of particular interest to adversaries or support uniquely significant data or services. In combination, security architecture reviews and vulnerability assessments provide system owners with recommendations to address identified vulnerabilities. DHS also works with the General Services Administration to ensure that contractors can provide assessments and other services to agencies that align with our HVA initiative. In the coming months DHS will be issuing an update to the BOD for securing HVAs that outlines required agency actions, senior agency leadership engagement, and an enhanced focus on the tracking and remediation of findings to further promote secure outcomes in alignment with the IT Modernization Report to the President.

Another BOD issued by the Secretary in 2015 directs civilian agencies to promptly patch known vulnerabilities on their Internet-facing systems that are most at risk from their exposure. The NCCIC conducts Cyber Hygiene scans to identify vulnerabilities in agencies' internet-accessible devices and provides mitigation recommendations. Agencies have responded quickly in implementing the Secretary's BOD and have sustained this progress. When the Secretary issued this BOD, NPPD identified more than 360 "stale" critical vulnerabilities across federal civilian agencies, which means the vulnerabilities had been known for at least 30 days and remained unpatched. Since December 2015, NPPD has identified an average of less than 40 critical vulnerabilities at any given time, and agencies have addressed those vulnerabilities rapidly. NPPD attributes this significant decrease in "stale" critical vulnerabilities to the clear cross-government expectation set up the BOD which enabled increased awareness across agency management teams which, in turn, prioritized agencies' efforts to quickly take action. By providing transparent reports to Agency executive leadership and engaging operational teams routinely on mitigation progress, NPPD continues to make progress in aligning its roles with regard to cybersecurity performance management and operational and technical assistance to help agencies find and fix vulnerabilities to secure their networks before an incident occurs. The progress made across Federal agencies to decrease the time it takes to mitigate critical vulnerabilities to Internet-facing systems has been encouraging. Because of the success of these efforts and the increased involvement of Agency executives to help drive positive organizational change and the prioritization of vulnerability management, NPPD is working to ensure the Federal government is meeting or exceeding industry standards and best practices related to vulnerability and patch management. Either through guidance, recommendations, or operational direction, NPPD will continue working closely with the Federal community to rapidly address vulnerabilities by shortening mitigation timelines where practical in order to further reduce agencies' exposure to cyber risks.

By sharing information quickly and widely, we help all partners block cyber threats before damaging incidents occur. Equally important, the information we receive from partners helps us identify emerging risks and develop effective protective measures. As required by the Cybersecurity Act of 2015, NPPD expanded a capability operated by the NCCIC, known as automated indicator sharing (AIS), to automate our sharing of cyber threat indicators in real-time. The Cybersecurity Act establishes the NCCIC as a civilian hub for sharing cyber threat indicators and defensive measures with and among federal and non-federal entities, including the private sector. AIS protects the privacy and civil liberties of individuals by requiring removal of known personal information not directly related to a cybersecurity threat.

AIS is a part of the Department's effort to create an environment in which as soon as a company or federal agency observes an attempted compromise, the indicator is shared in real time with all of our partners, enabling them to protect themselves from that particular threat. This real-time sharing capability can limit the scalability of many attack techniques, thereby increasing the costs for adversaries and reducing the impact of malicious cyber activity. More than 230 agencies and private sector partners have connected to the AIS capability. AIS is still a maturing capability and we expect the volume of threat indicators shared through this system to substantially increase. As more indictors are shared from other federal agencies, state and local governments, and the private sector, this information sharing environment will become more robust and effective.

Another part of the Department's overall information sharing effort is to provide federal network defenders with the necessary context regarding cyber threats to prioritize their efforts and inform their decision making. DHS's Office of Intelligence and Analysis (I&A) has collocated analysts within the NCCIC responsible for continuously assessing the specific threats to federal networks using traditional all source methods and indicators of malicious activity so that the NCCIC can share with federal network defenders in collaboration with I&A. Analysts from the Departments of Defense, Energy, Treasury, Health and Human Services; the FBI, and other agencies are also collocated within the NCCIC and working together to understand the threats and share information with their sector stakeholders.

Mitigating Cyber Risks

We continue to adapt to the evolving risks to critical infrastructure, and prioritize our services to mitigate those risks. For instance, the Department recently took action regarding specific products which present a risk to federal information systems.

After careful consideration of available information and consultation with interagency partners, BOD 17-01 was issued that directed Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities. The BOD called on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products within 60 days, and at 90 days from the date of the directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from federal information systems. This action is based on the information security risks presented by the use of Kaspersky products on federal IT systems.

The Department provided an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns, and Kaspersky submitted a written response. The Department wanted to ensure that the company had a full opportunity to provide any evidence, materials, or data that may be relevant. This opportunity was also available to any other entity that claimed its commercial interests will be directly impacted by the directive.

While the information and communications technology supply chain is not the source of all cyber risk, it presents an opportunity for creation of threats and vulnerabilities. Commercial technology is ubiquitous in federal networks, even those that handle the most sensitive information and support essential functions of the government. DHS—through its work with the Department of Defense and the intelligence community to identify key supply chain risks—has established a Cyber Supply Chain Risk Management (C-SCRM) initiative. Due to the increasing connectivity of the world and the growing sophistication of threats, this initiative will identify and mitigate supply chain threats and vulnerabilities High Value Assets.

Conclusion

In the face of increasingly sophisticated threats, NPPD stands on the front lines of the federal government's efforts to defend our nation's federal networks and critical infrastructure from cyber threats. Our information technology is increasingly complex and dynamic with interdependencies that add to the challenge of securing and making it more resilient. Technological advances have introduced the "Internet of Things" (IoT) and cloud computing, offering increased access and streamlined efficiencies, while increasing our footprint of access points that could be leveraged by adversaries to gain unauthorized access to networks. As our nation continues to evolve and new threats emerge, we must integrate cyber and physical risk in order to understand how to effectively secure it. Expertise around cyber-physical risk and cross-sector critical infrastructure interdependencies is where NPPD brings unique expertise and capabilities.

We must ensure that NPPD is appropriately organized to address cybersecurity threats both now and in the future, and we appreciate this Committee's leadership in working to establish the Cybersecurity and Infrastructure Security Agency. As the Committee considers these issues, we are committed to working with Congress to ensure that this effort is done in a way that cultivates a safer, more secure and resilient Homeland.

Thank you for the opportunity to testify, and we look forward to any questions you may have.

Mr. HURD. Thank you.

And now it's a pleasure to recognize the gentleman from Montana for 5 minutes.

Mr. GIANFORTE. Thank you, Mr. Chairman.

And thank you to the panel.

Mr. Powner, it's good to see you again. It seems like you're here monthly. And I appreciate your help in moving forward the IT procurement.

Mr. Zielinski, I would like to dive in a little bit into GSA's role in procurement, particularly as it relates to shared services. Could you talk a little bit about, to help the committee, what are shared services and what do you see as the benefits of mandating those for agencies where appropriate?

Mr. ZIELINSKI. So, in the broadest sense, shared services is an opportunity for us to, rather than having each agency independently build out a capability set, to be able to build those out in a centralized way.

It could be that it is a government-operated, government-built shared service, or it could be that it is a commercially offered solution. In working with the Office of Management and Budget, as well as with our own Unified Shared Services Management office, we are working to develop a series of shared services along the lines of business.

There's a lot of opportunities and benefits to this approach. First of all, there's significant cost savings. Secondly, as we talked about, the security posture, that ability for us to protect the shared service and be able to make changes to that individual or that one shared service and have all of the participants benefit across the government is significant.

Mr. GIANFORTE. Okay. And what IT services are already being procured under a shared services model?

Mr. ZIELINSKI. Oh, sir, there are a number. What I would like to offer is to be able to bring the full list, but I'll give you some examples here today.

Mr. GIANFORTE. Please.

Mr. ZIELINSKI. For one, we have a shared service offering that's in and around the implementation or the issuance of the PIV credentials, the HSPD–12 PIV credentials. That is operated out of GSA. There are 110 customer agencies with more than 750,000 credentials under active management.

That's an example of a very mature shared service that is utilized across government. There's shared infrastructure for agencies to be able to go to, common issuance sites. In addition, there are shared services for payroll, shared services for financial services. And we continue to build out other shared services.

And, again, I will bring back a more complete list of what those shared service offerings are.

Mr. GIANFORTE. Okay. So it sounds like shared services allow us to standardize procurement in such a way that various agencies don't have to roll their own, so to speak?

Mr. ZIELINSKI. Correct.

Mr. GIANFORTE. Yeah.

So there's cost savings. You mentioned earlier $50 billion of annual procurement. If shared services were fully implemented where appropriate, how big is the size of the prize in terms of savings?

Mr. ZIELINSKI. Yeah, I don't have an answer for that. You know, I think that as we are now going through the different lines of business and identifying those opportunities for shared services, we'll have a much better or more complete picture of what those savings opportunities are.

Mr. GIANFORTE. In instances where you have used shared services, how much savings resulted?

Mr. ZIELINSKI. It differs based upon the service itself. And, again, what I can do is bring back some more explicit information for each of these shared services as to where that is.

Mr. GIANFORTE. Okay.

So cost savings are one benefit. What impact does it have on security when a service is shared versus implemented individually by the agencies?

Mr. ZIELINSKI. So I would like to start, and I would also like to ask my partner, Ms. Manfra, to also add in as well.

One of the things that we're able to do is that, as each individual agency is building out a capability, that means that those individual agencies are also responsible for ensuring that they are patching and kind of doing the basic blocking and tackling that's necessary to secure the capability, and that if there is something that happens within the overall system that they have to respond to, that also means that they each individually would have to do that.

In a shared services instantiation, we have where there is a central group who is managing that security posture of the shared service. And that means that, when there is something that occurs or there is a need for us to make a change or to address a vulnerability, we are able to do that once and it is addressed for all of the customers of that.

Mr. GIANFORTE. And, again, I want to go back to my prior question. I realize you want to go collect more data, and I do want an accurate answer. But it seems like shared services presents an opportunity to standardize procurement, limit variability, increase security, and lower cost, all of which are good objectives.

Where is shared services on your priority list as you're working with agencies on procurement?

Mr. ZIELINSKI. So I will say that, going back to the IT modernization report, this is one of the core principles within the President's IT modernization report, is for us to look for those opportunities to build out shared services to be able to both speed the modernization but also to increase the protection. So it is one of the core priorities in moving forward with modernization.

Mr. GIANFORTE. And final question: Who should be managing these shared services within the government?

Mr. ZIELINSKI. The plan, as it stands today, is to look for managing partners based upon the capability areas. So, dependent upon what the business function or area is, that there is a role for the appropriate agency. So, in the case of HR shared services, OPM would have a significant role, as an example.

Mr. GIANFORTE. So, then, they could be a service provider to other agencies, if necessary?

Mr. ZIELINSKI. Correct.

Mr. GIANFORTE. Okay. Thank you.

I yield back, Mr. Chairman.

Mr. HURD. Ranking Member Kelly.

Ms. KELLY. Thank you.

The growing rate of sophisticated data breaches and cyber attacks in the private and public sector have heightened concerns over the security and strength of Federal IT systems.

And some of these devastating attacks succeed because Federal systems are dangerously outdated and obsolete. And I mentioned in my opening statement that nearly 75 percent of the Federal Government's IT budget is dedicated toward maintaining legacy computer systems.

Mr. Powner, why does it take such a large share to maintain those systems?

Mr. POWNER. Well, I think, historically, operational systems in the Federal Government get a pass. So when you look at that's something the lights are on and it's running and we're serving the mission, we might not be serving the mission efficiently, we might not be serving the mission securely, but it's gotten a pass over the years. That's been the biggest problem.

I think this committee, you know, going back to 2016, when we did the big report with the 8-inch floppy disk at DOD, helped raise the issue of how old and insecure and costly these systems are.

We are starting to make progress. The problem is that we still need firm dates to replace these systems where we actually turn them off. I mean, I agree with all the comments, that it's difficult to maintain and patch, there's unsupported software. But, ultimately, the security solution is turning them off and decommissioning them.

Ms. KELLY. I'm not trying to be comical, but because the systems are so old, do we even have the staff—we talk about the staff for the new systems and the workforce, but what about the staff to maintain these systems?

Mr. POWNER. Well, that—so it's very difficult. I know, personally, I do a lot of detailed work at IRS, and when you start looking at assembly programmers there, we're losing them left and right. We pay a premium to contractors to maintain. We pay other younger programmers who know modern language as a retention. It costs money to maintain these systems. And each year we go on, it costs more and more, and we become more and more insecure.

Ms. KELLY. And what happens if we just turn it off?

Mr. POWNER. Well, right now, we need a lot of these mission-critical systems to actually do the mission. You know, the IMF system at IRS, that's where we get $3.3 trillion in revenue through tax returns. It's critical.

Ms. KELLY. Uh-huh.

Mr. POWNER. Chairman Hurd's held hearings on the VA VistA system. I mean, we still need that to apply medical services to our veterans.

But, again, you know, that's why we need to keep them running, because they're mission-critical.

Ms. KELLY. Okay. Thank you.

The Modernizing Government Technology Act is a key component of this administration's continued effort to improve Federal technology by providing financial resources and technical expertise to agencies.

Does the MGT Act continue to be, you think, a priority for the Trump administration and OMB?

Ms. WEICHERT. Absolutely. The MGT Act and the Technology Modernization Fund are absolutely priorities for the administration.

And we've actually pulled together in the President's Management Agenda, which will be released next week and was hinted at in the President's budget in February, a wholistic perspective on how we tackle these issues, which is not purely the technology piece, as you have mentioned. It includes issues around data and data structure. It also includes very critical people issues.

We want to solve these issues wholistically, build on past successes, and we believe that the MGT and the Technology Modernization Fund will be great stepping stones toward the future of really pulling all of these dimensions together so that they are not siloed by function, where, you know, we have CIOs, you know, who, by the way, need more authority—and you all have done great work in FITARA to do that, and we support that. But we also need the human capital element, the financial element, the procurement element to be at the same table.

And so what we're laying out in the President's Management Agenda is that wholistic framework. It was why I was so eager to actually be here and share. Because one of the root-cause observations that we had when we looked at how government was tackling these issues versus the private sector, it was that lack of integration across function. And we plan to tackle that, leveraging these authorities that Congress has provided through the MGT Act and TMF.

And, by the way, we really hope the appropriators actually fund the TMF.

Ms. KELLY. Okay. Thank you.

Mr. Powner, can you comment on the steps that OMB is taking?

Mr. POWNER. Well, I think, clearly, the guidance that OMB just put out, you know, that's the right direction. And that guidance was very solid. You know, now the hard part is implementation. You know, we're really good at plans and guidance in this town, but we're not always good at getting things done and implementing them completely.

So let's do this right with the MGT Act, because we got savings out there. As Mr. Zielinski said, with shared services or still with some data centers, we can populate these working capital funds and really do MGT right.

Ms. KELLY. Thank you.

And I yield back.

Mr. HURD. Mr. Blum, you're now recognized for 5 minutes.

Mr. BLUM. Thank you, Chairman Hurd.

Thank you to our panelists for being here today.

Mr. Powner, your challenge is, in the next 5 minutes, to make me an expert on cloud computing. Cloud computing has been in the news lately with the Federal Government. Department of Defense, I think, is looking at going to cloud computing. I assume the entire government will be there at some point.

Can you talk to me about the efforts to go to cloud computing, A? B, financially, is that going to save the taxpayers money or not? And, C, I'm particularly interested in the following, and that is, will it be more secure or less secure or perhaps the same level of security that we have today, not being in the cloud?

Mr. POWNER. So there's all kinds of various aspects of the cloud. So, like, for instance, on our data center situation we have, when I say that some agencies by 2020 should get out of the business of data centers, that's because we have inefficient data centers that they're not going to optimize, maybe two-thirds of them. And what we could do there is we could host our existing applications in a cloud environment or on servers and infrastructure maintained by contractors who are cloud providers.

So that's one way that we could actually save money and have optimized data centers, by actually outsourcing all of it to the cloud.

We can also, too, in some of the shared service areas that we talked about, you can actually buy software as a service in the cloud from many of these cloud providers. And that's another way where we can save money.

However, there are some of these mission-critical applications like some of these homegrown systems that are critical to agencies' mission that you're not going to find that as a software, as a service, that we've got to actually just do the hard work and convert those old systems.

So cloud, there's a great opportunity. It's not the solution for everything. But there's substantial savings.

And from a security perspective, you know, if you really look, the intel community kind of led the cloud migration. We were concerned on the civilian side about having enough security. So if it was good enough for intel, it's probably good enough for a lot of others.

The other thing you could do is, through your contracting provisions—and we did work on this, looking at service-level agreements and contracts—you can specify the level of security you want from those cloud providers and actually dictate the level of security. So, in many ways, cloud services can be more secure than what we currently have.

Mr. BLUM. Do you think all Federal IT should eventually end up in the cloud?

Mr. POWNER. There are some aspects that won't be in the cloud because they're unique to agency missions, but there's a large portion that could end up being in the cloud.

But there are these pockets of unique applications that we do that no one else has that we have to do the hard work and convert those to more modern platforms and modern software.

Mr. BLUM. Where are we at today in this journey to the cloud?

Mr. POWNER. So that's a good question. We're doing some work for this committee where we've done prior works, and we try to measure it as a percentage of budget or IT spend, and it's very difficult. You know, we did this work a couple years ago, where agencies varied from 2 to 7 percent of their IT budgets were in the cloud. That's improved somewhat. But it's very difficult to give you a good, hard number right now. We're working on that for this committee.

Mr. BLUM. Thank you.

Ms. Weichert, is it?

Ms. WEICHERT. Yes.

Mr. BLUM. OMB, how involved are they in this migration to the cloud?

Ms. WEICHERT. So it's a great question, and it is actually one of the priorities that we're laying out as part of the President's Management Agenda. Now that the Federal CIO is in place, it is on her top priority list.

And we're working closely with GSA and the centers of excellence on the implementation. They've already met to put together tiger teams in terms of cloud email adoption, and they're looking at other areas where commercially available solutions are already in place, secure, and working at some agencies, to elevate the lessons from those and extend them across government.

But ultimately the test, to the question that you asked earlier around which things should migrate to the cloud, it's essentially going to be dependent on the mission; the service aspects, so how well we can serve the needs of our citizens and the American people; and then the stewardship aspects of financial stewardship. So we're really going to be looking at balancing those three items.

Mr. BLUM. Thank you.

Mr. Zielinski—I hope I pronounced that right—this is kind of interesting. The centers of excellence, can you just briefly tell me about that and that effort?

Mr. ZIELINSKI. Certainly. Thank you for the question.

Going back to some of the things that Mr. Powner mentioned, as agencies are making these decisions about their strategies for moving to the cloud or considering the cloud, the centers of excellence are places where we bring together technical expertise, the engineers and others who understand the dynamics of matching those business applications and those business functions to where they best lend themselves to a cloud application, whether that software is a service or platform is a service, and then help agencies to find acquisition strategies for them to be able to move.

So there's a lot of direct assistance that those centers of excellence provide to a customer agency, and they do that through bringing together the expertise, as Ms. Weichert said, being able to make sure that we have all of those functions working hand in glove, the technical expertise as well as the acquisition.

Mr. BLUM. Is it more of a planning function or more of an execution function, the centers of excellence?

Mr. ZIELINSKI. It's absolutely an execution function, sir.

Mr. BLUM. Because I agree with what Mr. Powner said earlier about we're good at planning, not so good at following through.

Thank you very much. I am out of time and I yield back.

Mr. HURD. I now recognize the ranking member.

Ms. KELLY. I just have one quick question and not for Mr. Powner.

How long have all of you been in your positions you're in now?

Ms. MANFRA. I was appointed in June of last year, ma'am.

Mr. ZIELINSKI. I've been with GSA for 2 years.

Ms. KELLY. In the position you're in now?

Mr. ZIELINSKI. Six months.

Ms. WEICHERT. The Senate confirmed me on Valentine's Day of this year.

Ms. KELLY. All relative newbies, okay. No insult to you, I just knew you'd been around. Thank you.

Mr. HURD. He's been there forever, I think is the right answer.

Mr. Zielinski, can we follow up on the centers of excellence. I recognize myself for 5 minutes. How does this program differ from 18F?

Mr. ZIELINSKI. So thank you for the question, sir. The 18F has those technical experts that the centers of excellence can actually tap into. So as I talked about bringing together the different discipline areas to be able to bring to bear on a particular agency problem set and to assist them in being able to understand the dynamics of their business case and how they can move forward, 18F, as an organization, would be one of the areas into which the centers of excellence can reach to bring that technical expertise to the table.

Mr. HURD. Got you. And how do we ensure these centers of excellence, other than having GAO white glove it, how do we ensure that these don't duplicate efforts that are going on in the rest of the government?

Mr. ZIELINSKI. So going back to the agenda that has been laid out by the administration in and around starting with the IT modernization report as well as with the President's Management Agenda, it's a very tight weave in terms of ensuring that there's a collaboration across all those functional areas.

And there are many opportunities for those functional areas to be brought together to ensure that we are all bringing to bear the best talent and that we're also not duplicating effort, sir.

Mr. HURD. Good copy.

Ms. Weichert, one of the things that is still frustrating, and I'm glad Mr. Powner alluded to this in the beginning of his remarks, is CIO authorities. We can't hold CIOs accountable if we don't give them all the power they need. FITARA gives them that authority, but in many places the agency CIO doesn't have the complete budget authority of those—of that entire operation.

And Transportation is an example. I think they have nine CIOs, people with the title, nine CIOs, $3 billion-plus budget.

Can we reprogram the funds from those various sub-CIOs into—under the Federal—under the agency CIO in order to streamline that budget authority?

Ms. WEICHERT. So not being an expert on appropriations, I want to caveat and say that I would love to answer that in more detail after conferring with some of our budget folks. But what I can say is absolutely agree with your frustration. It's something we in the administration share and are looking very closely at how do we address.

I think in the President's Management Agenda we are laying out how all of the components of the various authorities across government, how they work together and how they align together, and to avoid duplication, while giving the maximum elevated level of capability to the CIOs.

I think the Technology Modernization Fund and the MGT, in providing new capabilities around working capital funds, that is a place we are going to start and are already exploring ways that we can work with agencies to help them focus and target resources towards the highest priority projects, as Mr. Powner has suggested.

In terms of getting additional capabilities, I think the authorities are different in terms of transfer and how they can use their working capital funds, that I wouldn't want to give you an across-the-board answer.

Mr. HURD. But would you have heartburn if we were to reprogram some of these to ensure that the agency CIO had all the budget authority for IT spend across that network?

Ms. WEICHERT. So I haven't studied that specific issue.

Mr. HURD. Okay. That's a fair answer.

Ms. WEICHERT. But what I can say is we are absolutely in alignment in terms of the idea that the CIO for the broad agency needs to have all the capabilities and tools to make these very profound investments.

And the more we can align to the way the private sector works, where you've got a general manager of a division or an agency, and their C-suite includes the chief information officer, the chief financial officer, the chief people officer, and, where appropriate, the procurement officer, they need to all be there in lockstep.

Mr. HURD. And the CIO. I think you said that.

Ms. WEICHERT. I said that first, yes.

Mr. HURD. Okay, first. Okay. Gotcha. Gotcha. I agree. And my teams would get mad because we're talking about how do we change the FITARA Scorecard to penalize agencies that don't have the Federal CIO reporting directly to the agency or deputy agency head.

We've asked everybody why, what's going on, why is that the case? We've gotten a lot of excuses: "Oh, it's kind of already there." Well, if it's already there, then change the damn structure. And so we are looking at having that be reflected in the FITARA Scorecard.

Mr. Powner, do you have any opinions on the reprogramming and giving complete budget authority to the CIA—CIO? Let me rephrase that. The CIO, not the CIA. I don't want anybody to get mad and run an ad against me.

Mr. POWNER. I think the first step is that we understand all the IT spend. I think many CIOs, we don't even know the full totality of what we spend at these departments and agencies. So once we understand that, I do think the CIOs should control that more.

It's okay, too, if there ARE some business units that control it and they act in partnership, where the CIO is working with those business units to spend it appropriately, to oversee it the right way and that.

So I think there's probably even some blend. I think right now if we did it completely whole hog, you have complete budget authority, the whole bit, I don't know if that would—maybe we need to shock the system as you're intending. That's one way to do it.

Mr. HURD. Your word, not mine, sir.

Mr. POWNER. But the other way to do it is to have some type of blend where we know the entire spend and the CIO has a role, whether they control every dollar or not, but they're still responsible for governing over it. We've got too much IT spend that we don't have IT people on it.

Mr. HURD. You reminded me of something I was going to ask.

And, Ms. Weichert, this may not be something on the top of your mind.

Or, Mr. Zielinski, I think this is outside of your scope.

The Department of Defense recently made the decision to not publish their IT amount. I believe it was in a recent—was it an OMB report? What was it? The analytical prospectus. It said: Hey, we're going to stop showing DOD's number on IT along with everyone else.

So we went from spending, the Federal Government spending $90 billion to $40 billion, and they said, you know, asterisks, fiscal year 2018, it was roughly $50 billion.

Do you have any insight into that decision, that process? And we will be bringing—again, not to, you know, show our hand—but we'll be bringing DOD for the next FITARA Scorecard hearing to have them answer that directly. But I'd welcome your thoughts.

Ms. WEICHERT. Yeah. Unfortunately, that was prior to my being confirmed, so I wasn't read in on that particular decision.

Mr. HURD. When you're talking to them——

Ms. WEICHERT. I will note it.

Mr. HURD. —tell them this committee is interested.

Ms. WEICHERT. I will share that.

Mr. HURD. And I'd love to have the answer prior to—should I introduce these into the record?

So, yeah. The analysis in this chapter excludes the Department of Defense and classified spending, which in fiscal year 2008 was $42.5 billion, or 44 percent of the IT budget. So we're going to start showing only 66 percent of the budget as a whole number, which seems a little odd to me.

Ms. Manfra, one of the things I want to do with the FITARA Scorecard is transition it into more of a digital hygiene scorecard as well. I think the elements, as Mr. Powner has talked about, we've got to continue to double down on those issues.

But I think being able to highlight at the macro level good digital hygiene is important. I think the inclusion of the MEGABYTE Act on that was one of that. Do you know all the software that's running on your system? And I think only three were able to answer yes, which is pretty shocking. And, again, these are self-reporting numbers.

So what are some of the areas that you think that we should or could be exploring when it comes to digital hygiene and how we look across that over the entire enterprise?

Ms. MANFRA. So I think, first of all, I think that's a great idea, to include that. Frankly, shining a light on some of these basic practices has been useful in agencies prioritizing.

So I briefly alluded to the critical vulnerability patching. What we saw through years of assessments was just continued poor patch management programs. Some of it does have to do with legacy systems and all that.

But what we decided to issue, our first binding operational directive, was actually to require the time to patch a critical vulnerability down to 30 days.

And the important way, though, that we were able to be successful, I think, with this and with other directives and other guidance that we provide is that we can independently validate. We're not relying on self-reporting. And so the more capability that DHS is deploying—in this case it's the external scanning that we're doing of all internet-facing devices—that we can say, no, I can see that you haven't actually patched.

The good news story is that when we—I think fiscal year 2014 average time to patch was somewhere in excess of 200 days for critical vulnerabilities, which is bad. After the directive—and it continues, which shows how these things change behavior—we're averaging in the 10 to 15 days.

And so it's helping them prioritize their very limited resources by focusing on known issues, and that's what we want to continue to do, but it's also important that we can independently validate this.

You talked about knowing what software on your system. So the Continuous Diagnostics and Mitigation Program that we've been deploying, the first phase is hardware and software asset management. And we've learned a lot through that program in what agencies thought they had on their network was not exactly what we found that they had on their network after deploying these.

And I know in one sense it's frustrating to sort of be in that environment, but at least we're in a position now where we do know. We know what's connected to the network and as we deploy more tools.

And as a side note, this program actually is also very cost-effective, and we've been able to identify that I think it's 75 percent cost savings off of schedule—if they had bought these on Schedule 70.

So we're deploying common tools that are identifying what and who is on networks. And I believe that this will fundamentally transform the way that we do, in the first case, vulnerability management for the government, but eventually we will get to event management and ongoing authorization in those programs.

But it has to be through the deployment of these standardized tools that then feed data back to an agency CIO and DHS so that we can, through automated sensors, understand where they are.

Mr. HURD. Would you have security concerns of publishing that number of how long it takes to patch software, like the average it takes to patch software from agency from agency?

Ms. MANFRA. I don't know how——

Mr. HURD. You can take time to think about it.

Ms. MANFRA. Yeah.

Mr. HURD. It's just I think that's an element that, self-reporting, we can establish a letter grade based on what are industry best practices. Is a week an A? Two hundred days is definitely an F, right? Where that's something that we could package and keep track of and make sure that we're continuing to shine a light on.

Ms. MANFRA. Absolutely, sir. And there's a few other things that we've identified as very common practices that we're focusing our guidance on. And we'd be happy to work with you on how we can improve those practices.

Mr. HURD. And before we get to the gentleman from the Commonwealth of Virginia, my last question is, one of the things that I've—in the 3–1/2 years we've been doing this together, we've asked a lot of questions about, are you doing technical vulnerability assessment, penetration testing? And a lot of agencies have said yes, and then you find out after the fact they're just doing a scan, that they're not bringing a third-party system, a third-party vendor to come in and do that testing.

Your organization has been doing that. Have you seen an increase in that as a best practice?

Ms. MANFRA. So you're right, there isn't a very common definition of what people mean by penetration testing. You know, as I noted, we do passive scanning, but that is to identify one set of issues.

We also do our risk and vulnerability assessments, which is penetration testing, which is actively going and trying to identify and exploit vulnerabilities. That's what we would consider.

We haven't previously taken statistics on what agencies are using penetration testing. I can tell you that just in the last fiscal year, we did 42. We focus, prioritize high-value assets. So we go through all of the high-value assets to do a full risk and vulnerability assessment, which includes a penetration test as well as a report to them. But we could definitely follow up on that.

Mr. HURD. Well, we'll be asking the agencies this question, so when we collect that information we'll share it with you so that you're aware.

Ms. MANFRA. Thank you, sir.

Mr. HURD. Now I'd like to recognize the gentleman from the Commonwealth of Virginia, the ranking member, Mr. Connolly.

Mr. CONNOLLY. I thank my friend.

And welcome to our panel.

And thank you both to Mr. Hurd and Ms. Kelly for their leadership of this subcommittee and on this subject matter. We're really fortunate to have Members who care about the subject matter and delve into it. It's actually rare. You'd think more Members would be involved in IT, but they actually aren't, for various and sundry reasons.

And so one of the great pleasures of serving on this committee is that—and Mr. Meadows is not here, but the four of us have really worked seamlessly, in a nonpartisan way, to try to help rationalize Federal IT policy. And I think for all four of us, it doesn't matter whether it's a Democrat or a Republican administration, we want it to work.

And so, in that spirit, welcome.

Ms. Weichert, in March of last year the White House announced the Office of American Innovation. And after that, OAI was credited with a whole bunch of projects as large as pushing the overhaul at the Veterans Administration healthcare IT system, setting the policy for the Federal Government's adoption of AI, and presumably implementation of FITARA, data center consolidation, moving to the cloud, empowerment of CIOs, and so forth.

Now, under the E–Government Act of 2002, normally that role would be played by the Federal CIO. Now that presumably we're going to have a Federal CIO, what is OAI's role going forward, and how does OMB play a role in all of this as well?

Ms. WEICHERT. I think it's a great question, and we are working in lockstep across the administration to set out a focused agenda for all the elements around not only IT modernization, but the other enabling capabilities around data transparency and accountability, as well as the people dimensions of that.

And OAI did a great job providing catalytic capabilities in getting a lot of these activities started. But what's been included in the President's budget in February and what will be rolled out next week in the President's Management Agenda is the comprehensive go-forward plan.

We do have a Federal CIO, an outstanding leader from the private sector who has done execution of change in complex, highly regulated environments in the financial services and other industries, who's really here to help continue to carry that torch.

I think a lot of the activities that have been enabled by the MGT Act and the TMF are stood up. The Federal CIO actually met earlier this week with the members of the IT Modernization Fund Board, and they did a dry run, so that when appropriations come—I'm hoping they're coming soon—that the board will be prepared to act quickly.

We continue to work very closely with OAI in terms of helping shape the strategy and bring to bear the best thinking of the administration and also marshal resources outside of government to provide insights that might be helpful in our journey.

But we in OMB are really leading the direction with the President's Management Agenda and bringing the executive branch along. And I look forward to having you all get to see what we're putting together that's going to be in the PMA launch next week.

Mr. CONNOLLY. So I know that the chairman talked about maybe broadening the current FITARA Scorecard at some point to a digital hygiene scorecard. I would be supportive of that once we make more substantial progress on implementation of what's in front of us, because we've seen some backsliding. You know, DOD, the Big Kahuna, got an F. And so we want to see more progress, but we can't really see it without leadership coming from your office.

I assume, but let me ask, you are committed to the metrics set in the law, FITARA, and the tools, allowing us to try to facilitate that, that MGT, just passed into law, also gives agencies, to facilitate implementation of the law.

I assume you're trying to push agencies to meet the metrics set for them in the law.

Ms. WEICHERT. Absolutely. And I think the focus historically, that has been very siloed. In a lot of cases some of the challenges around FITARA implementation and some of the things measured in the scorecard hit root cause issues that were underlying those things. In a lot of cases, people issues are part of the problem.

Mr. CONNOLLY. Yes.

Ms. WEICHERT. In some cases data and even the ability to see the problem is part of it.

So part of what we want to do is actually use the broad management table to really shine a light on those issues. And to the extent the scorecard needs to evolve or mature, we'd be very happy to take input from GAO and work with Congress on that. But we are very supportive of the spirit of FITARA and moving forward with that.

And I guess the last thing I'll just say is, my perspective in the private sector, if you've got a broad failing to meet the needs outlined in a strategic plan or a set of metrics, it's incumbent upon the person who's accountable for those, especially if it's me, to really understand are there root cause issues that are preventing us from doing that and then addressing those as well.

Mr. CONNOLLY. Yes, I couldn't agree with you more. And like you, I come from the private sector. I spent 20 years as a corporate officer. And what I learned in the private sector and the public sector is, if the boss doesn't care, neither do I.

Ms. WEICHERT. Right.

Mr. CONNOLLY. I'll give it lip service.

Ms. WEICHERT. I care. I care a lot.

Mr. CONNOLLY. Exactly.

But they need to feel pressure. They need to know I'm going to be evaluated by the boss on implementation, on meeting those metrics.

And the other thing, and then I'll be quiet, but with respect to personnel, we've got to empower, in Latin we call it primus inter pares, the first among equals in CIOs. There has to be a primus CIO who's got the responsibility, the accountability, and the power to make decisions. They've got to be empowered, and everyone has to know that.

If the CIO of an agency is reporting to the deputy assistant Gromit in the basement, that does not escape the attention of everybody else. And I might give lip service, but I know he or she doesn't really have the boss' attention.

We elevate the issue—I mean, we elevate the role of that person and the stature of that person, we elevate the issue and its importance in everybody's eyes.

I commend that to you as a reform. It doesn't cost a lot of money, but I think it would have a profound effect on performance and would save a lot of money for agencies over time and make us a lot more effective.

Thank you, Mr. Chairman.

Mr. HURD. Thank you, sir.

And I failed to spend some time on MGT, so I have a few questions. And, Ms. Weichert, they're probably best for you.

The agencies are still planning to present their implementation plans of the MGT working capital fund on the 27th of March. Is that correct?

Ms. WEICHERT. That is correct.

Mr. HURD. And will you be able to share those with us?

Ms. WEICHERT. So we will be able to share the status on the working capital funds early this summer. So we are actively working with the agencies to understand what specifically their needs are in terms of implementing on that.

So we already have a number that are well on the way of implementing it. We have identified some challenges related to transfer authorities that we need to work out. And we'll actually be coming back to Congress with some thoughts about ways to streamline what's needed to actually make it work as intended in the legislation. But we will be coming back imminently.

Mr. HURD. The sooner you come to us on that, we'll do everything we can to help, because I think it's important by the end of this fiscal year to have some money deposited in those funds at a handful of agencies to be sure that it's working.

Ms. WEICHERT. We absolutely agree, yes.

Mr. HURD. Mr. Powner, do you think we can do that?

Mr. POWNER. Definitely, definitely. And we'll continue to work with you. I know that's one of the things we want to focus on the scorecard, too, as we evolve that, to look at the establishment of those MGT funds and the accountability, who's in charge of those and that type of thing.

Mr. HURD. Because if you are able to deposit money in your MGT working capital fund, it shows a culture of modernization, and I think that's important to monitor and focus on.

I'd like to thank our witnesses again for being here today. The hearing record will remain open for 2 weeks for any member to submit a written opening statement or questions for the record.

If there's no further business, without objection, the subcommittees stand adjourned.

[Whereupon, at 4:26 p.m., the subcommittees were adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Representative Robin L. Kelly
Post-Hearing Questions for the Record
Submitted to Margaret Weichert

OGR Hearing "State of Play: Federal IT in 2018"
March 14, 2018

1) A recent article in Netgov (http://www.nextgov .com/emerging-tech/2018/02/it-costs-taxpayers-41-phone -call-irs/ 145870/) pointed out that the IRS spends approximately $41 for each phone call and $67 per in-person visit. How can we better leverage technology, including artificial intelligence, chat bots, mobile services, websites and related to improve response time and reduce the cost of government customer service?

   Response: One of the primary drivers of the President's Management Agenda (PMA) is IT Modernization, which specifically envisions using leading technology services and capabilities to modernize government with the goals of 1) improving mission delivery; 2) improving government customer service; and 3) better stewarding taxpayer dollars.

   Specific cross-agency priority goals (CAP Goals) provide concrete action plans for areas in which the Administration and Executive Branch Agencies will focus to leverage IT to enhance service. Three relevant goals include:

   - **Modernizing Government IT (CAP Goal 1)** – which includes investments in core infrastructure
   - **Data, Accountability and Transparency (CAP Goal 2)** – which includes initiatives around artificial intelligence and other data tools
   - **Improving Customer Experience (CAP Goal 4)** – which focuses on how to enhance end-to-end experience including response times, web experience, etc.

For more detail, please refer to the information at https://www.performance.gov/PMA/PMA.html.

2) Building on this theme, the President's Budget for FY19 calls for "improving the customer experience with Federal services," as well as "modernizing IT to increase productivity." What is your vision of how the Federal government can use technology to increase productivity and improve customer experience?

   Response: The entire goal of the President's Management Agenda is to focus resources from across agencies and across functions to better support the needs of our 21st Century mission, service and stewardship needs. IT Modernization is at the heart of making the transition to a government that meets the needs of the 21st Century. Authorities provided in the Modernizing Government Technology (MGT) Act, provides the needed first step to allow agencies to flexibly address the IT Modernization capital investments required. Building on those authorities, the CAP Goals identified in the PMA identify specific areas where the Administration is focused on addressing structural barriers to change. Specific areas of focus include:

- IT Modernization Report Opportunities – specific focus on cyber vulnerabilities
- "Cloud Smart" – adoption of efficient and effective cloud technologies where appropriate
- Skilled IT Workforce – adding the appropriate skills to help lead and manage the IT transformation

Again, additional information and detail on this vision for IT Modernization is available online at https://www.performance.gov/PMA/PMA.html.

Office of Congressional and Intergovernmental Affairs

Subcommittee on Information Technology
House Committee on Oversight and Government Reform
"State of Play: Federal IT in 2018."
March 14, 2018

Questions for the Record for Deputy Assistant Commissioner William Zielinski, GSA

Below you will find Representative Kelly's question and Deputy Assistant Commissioner Zielinski's response to it.

1. **What is the status of the $50 billion Enterprise Infrastructure Solutions (or, EIS) contract? Do you feel like agencies are taking the steps necessary to transition under current timeframes? Do you think they are adequately prepared to transition to EIS?**

   GSA is completing the implementation phase of the $50 billion EIS contract and will begin the initial task order award and enterprise transition phases. The transition phase will move services to EIS from Networx and other Federal Government telecommunications contracts. The completion of the implementation phase is contingent upon each contractor finishing and testing their business support systems, as well as agencies completing their solicitations and awards. Even as implementation is nearing completion, agency solicitations are already being released, and a high percentage of the overall anticipated solicitations among medium and large agencies are in process. One hundred percent of Agency Transition Plans have been submitted to GSA, and EIS solicitation activity over the last 6 months suggests agencies are taking the necessary steps to transition.

   As of late May, GSA is supporting the development of approximately 60 agency solicitations through the Transition Ordering Assistance program. In total, GSA expects approximately 180 solicitations for those agencies purchasing above $1 million per year through GSA. Agencies have forecasted that most of these solicitations will be released in the fourth quarter of fiscal year (FY) 2018. While GSA cannot speak for agencies, the complexity of transitioning creates hurdles for agencies completing their solicitations.

   Telecommunications transition is complex for Federal enterprises and can involve significant resources from both the agencies and telecom providers. With the release of the Report to the President on Federal IT Modernization in December 2017 and the issuance of the President's Management Agenda (PMA) in March 2018, many agencies are reviewing their current transition plans to ensure that they are appropriately leveraging the EIS transition as an opportunity to modernize their network infrastructure. The existing telecommunications contracts (e.g., Networx) expire in mid-FY 2020, and GSA will continue to work with agencies as they complete their transition and leverage EIS for their modernization efforts.